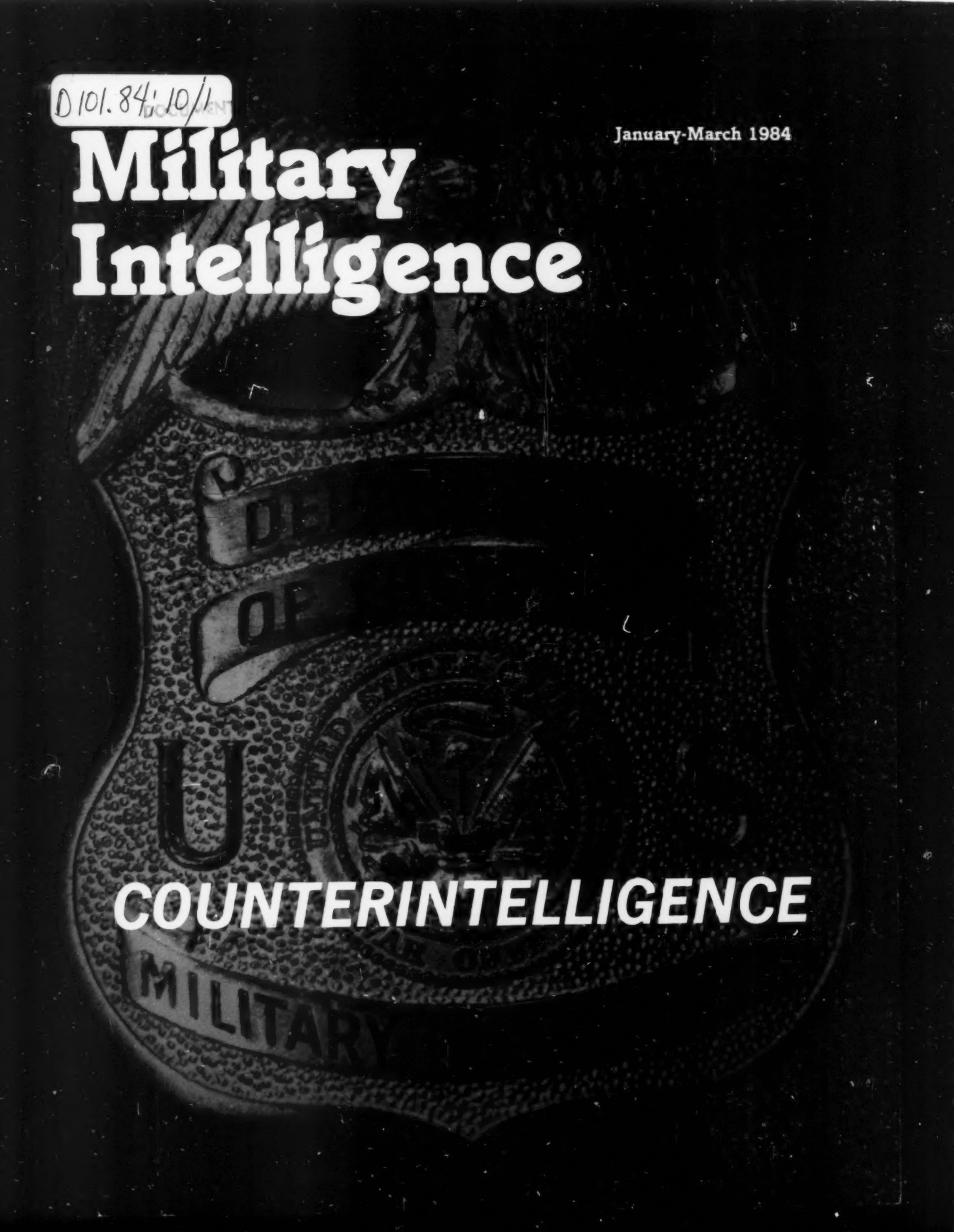
# Military Intelligence

January-March 1984




## COUNTERINTELLIGENCE

## Features



***Military Intelligence*** is an authorized publication of the U.S. Army Intelligence Center and School, Fort Huachuca, Arizona, published quarterly under provisions of Chapter 5, AR 310-1. Unless specifically stated, material appearing herein does not necessarily reflect official policy, thinking or endorsement by any agency of the U.S. Army. Use of funds for printing this publication was approved by Headquarters, Department of the Army, December 1975. Use of the third person pronoun "he" and any of its forms, as used in this publication, is intended to include both masculine and feminine genders. ***Correspondence*** with ***Military Intelligence*** is authorized and encouraged. Inquiries, letters to the editor, manuscripts, photographs, and general correspondence should be sent to ***Editor, Military Intelligence***

# Military Intelligence

From the Home of Intelligence

Volume 10 Number 1 January-March 1984



## Departments



## Staff

**Editor:** *2nd Lt. Frederick J. Britton*
**Assistant Editor/Departments:** *Sp5 Robert A. Kerr*
**Art Director:** *Virginia C. Harris*
**Illustrator:** *Sp5 Peter G. Varisano*
**Plans and Administration:** *Sp5 Bernard L. Jamison*
**Typographer:** *Sp5 Wasena J. Leavelle*

Magazine, U.S. Army Intelligence Center and School, Fort Huachuca, Arizona 85613. Telephone Autovon 879-3033, commercial (602) 538-3033. ***Subscriptions*** to ***Military Intelligence*** are available through the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. A check or money order, payable to Superintendent of Documents, must accompany all subscription requests. Subscription rates are $9.50 domestic (including APO and FPO) addresses, and $11.90 for foreign addresses. ***Controlled Circulation*** postage paid at Washington, D.C. **ISSN 0026-4028**

The Counterintelligence Shield graces our cover this issue. The ***MILITARY INTELLIGENCE*** staff wishes to thank members of the Counterintelligence Division, Department of Human Intelligence, USAICS, for their immeasurable help in getting this issue to press.

# from the Commander

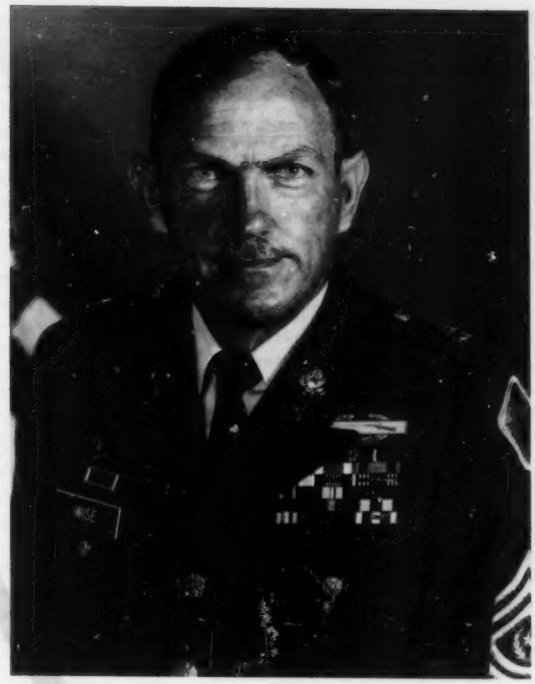
**by Maj. Gen. Sidney T. Weinstein**

The human element remains one of the keys to successful intelligence in peace or in war. The last issue of **Military Intelligence** focused on the fast moving world of high technology. With all of these advances, it is important to remember that where the machines leave off, an intelligence professional must be there to provide the extra effort, careful analysis or skillful collection.

The growing strength of the "human side" of intelligence becomes apparent when I talk to the military intelligence professionals here at the Intelligence Center and in the field. It is important to recognize that as we place more demands upon equipment to meet intelligence requirements, we also place more demands on intelligence soldiers. Today's intelligence soldiers are required to analyze large volumes of information and determine what to exploit and how to best exploit it. Successful counterintelligence, deception operations and intelligence analysis require well trained intelligence professionals. Today's M.I. soldiers must be the best ever. If we continue to sharpen skills and improve training, they will be the best.

The Intelligence Center and School is committed to meeting this growing challenge. Units in the field are facing the same challenge, and many have had brilliant success. Communication between the school staff and the professionals in the field is the key to continued success. Keep your ideas flowing to the "Home of Intelligence." Our branch will improve, we'll all do our jobs better, and most importantly, the U.S. Army will be provided with the best intelligence possible.

# from the CSM



**by CSM Sammy W. Wise**

Counterintelligence provides commanders with the capability to cue other sensor systems to defeat deception, to observe and report on areas of interest, and to provide direct insight into enemy intentions.

The value of counterintelligence and the indispensible part it will play on tomorrow's battlefield is not debated. Considering the employment of high technology by enemy forces, and the predictable fluid characteristics of the next ground war, CI will undoubtedly be one of the most reliable and available means of knowing the enemy. If we want to win the battles, both large and small, we cannot afford to ignore the readiness posture of our soldiers working in the CI discipline.

The counterintelligence agent (97B) is the key to successful CI operations. The expertise of these soldiers crosses several lines; counterintelligence, operations security, communications countermeasures, counter-human intelligence, counter-signal intelligence, and counter-imagery intelligence. They can support commanders with security, rear area Intelligence Preparation of the Battlefield, signal security, CI investigations, and countering the terrorist threat. This diversity of talent allows them to be active participants in any intelligence operation.

Regrettably, our 97B soldiers, in addition to being one of the most versatile intelligence assets, are also often the least understood. The misutilization problem of the 97B surfaces during every Branch Training Team visit to the field, and is a common topic of discussion among all 97B soldiers. Reports to me indicate they constantly exceed their fair share of being assigned to nonintelligence related duties, regardless of rank. I consider this not only an injustice to the men and women holding MOS 97B, but also to the unit to which they are assigned. We have a moral and contractual responsibility to gainfully employ all of our soldiers with the ultimate goal of mission accomplishment and professional development of the individual. Anything less is unacceptable in today's Army of excellence.

I fully realize that there are soldierly duties and tasks which need to be done in every unit, and at every echelon, which do not relate to technical job descriptions. All professional soldiers have done them throughout their careers, and will continue to do them as required. I certainly do not perceive it as a disservice to the 97B just because he or she is assigned to those duties. If it is because we, as managers, are unaware of their potential professional and technical contributions to the unit, or because we are undecided as to how to properly utilize their skills as 97B, then we are at fault, and they deserve better.

I am convinced that the problem of misutilization of 97B soldiers exists and is wide spread. I am also convinced that we can deal with this problem in a manner of benefit to both our units and the individuals concerned. The solution is relatively simple, and can be implemented at little or no cost in either time or money.

First, commanders and supervisory personnel must make a special effort to totally familiarize themselves with the skills in which 97B soldiers have been trained. Following that, they must incorporate those skills into the unit's intelligence operations so the 97B becomes an integral part of the intelligence team. This philosophy can be applied in both real world and training situations. With the same imagination used in developing training scenarios for other MOS, an artificial environment can be created in which the 97B can refine and maintain his skills to the extent that he too will be prepared to go to war. One advantage that participating in a training exercise has over conducting real world operations is the inherent flexibility to be able to amalgamate both technical and common soldier tasks into the scenario as required performance.

Commanders and senior CI agents have the responsibility to train new or less experienced 97B soldiers, just as in other MOS. This obligation is not waived by the fact that the CI agent may be working in an isolated duty location, or is deeply involved in performing only one aspect of his MOS. The total spectrum of CI skills must be maintained to ensure the 97B remains a versatile intelligence asset to the unit commander.

97B10 soldiers, in particular, need to concentrate on fine tuning their professional skills so they are ready for 97B20 transitional training. We lose far too many of these soldiers because their field experience has been less successful in preparing them to meet this advanced academic challenge.

In summary, the 97B soldier is considered to be a highly qualified, dedicated member of the U.S. Army. He or she has the same aspirations and expectations as all professional soldiers, and that this is to become a respected and productive member of the U.S. Army. To this worthwhile end, we must provide all the encouragement and assistance we can.

Take care of the soldiers.

# FEEDBACK

**Editor:**

*Mr. Colanto's article was a neatly compacted version of the field manual on Intelligence Preparation of the Battlefield. I am very much in favor of this concept, however, there are three areas which require special consideration.*

*First, is the relationship of the intelligence analyst and the supporting terrain team. The terrain team utilization is dictated very heavily by the needs of the engineer topographic battalion and, as such, terrain information requirements of the intelligence analyst are lower on the priorities list. Also, to date, we have not been able to coordinate the activities of each element into a long-term dialogue. Rather, piece-meal efforts are staffed depending on what aspect commanders want to focus on in a given week.*

*Secondly, is the required input from the Air Force weather team. This is an area which so far has not yielded the details necessary for an accurate assessment of enemy intentions in light of weather variables. As yet, no one is being held accountable for weather templates as described in Mr. Colanto's article. At best, weather teams provide only climatic summaries and general weather pattern predictions.*

*Lastly, IPB has been around for several years and hopefully continued publication will finally extoll its virtues. Unfortunately, there are those who are still not familiar with the IPB precepts and mis-directing the functions of IPB much to the expense of the intelligence analyst.*

**CWO 2 Anthony C. Mays**
Order of Battle Technician
CTOC Support Element (Corps)

**Editor:**

*I have been reading* ***Military Intelligence*** *magazine for nearly one year now and so would like you to know that I consider it one of the most interesting publications that I do read and that I am pleased that it is available to the civilian community.*

*By the way of explanation, I have no formal ties in any way to the military, much less the intelligence community. I have been interested in military history for a very long time and am especially interested in signal intelligence and have developed a very nice library of books and periodicals in my home, using military-grade radio receivers and auxiliary equipment, and maintain listings of frequencies and traffic passed on those unencrypted signals that I do work.*

*I did spend three years in the U.S. Army, from February, 1966, to February, 1969, and held MOS's 05C40, and 31M40 upon separation from active duty. So, I do have prior experience in my current pursuits. Your publication, along with* ***Signal****, published by Armed Forces Communications-Electronics Association, provides me with information on current and projected capabilities and equipment as well as theory and doctrine and I must say that it is all very interesting and I find myself somewhat envious at the current avenues of endeavor being pursued in signals intelligence and exploitation.*

*I would like to know if back issues of* ***Military Intelligence*** *might be available for purchase so that I could expand my library accordingly. I'd certainly appreciate your advice, and instructions, as to how I might obtain one copy of each back issue available.*

*While I suspect that* ***Military Intelligence*** *is somewhat sanitized for public consumption, I am still somewhat surprised at the amount of material published because I would personally consider everything about the subject very sensitive and not acceptable for public dissemination. I handled quite a bit of sensitive communications and subject matter during my active duty days and theory, policy, and even all equipment used was not talked about outside our work areas and so I must admit that I am sometimes uneasy when reading about docrine, tactics, and equipment as set forth in the pages of* ***Military Intelligence****. I guess times have changed.*

*In closing, I would again like to let you know that I do enjoy your magazine and I hope it continues to be as informative and thought-provoking. Thank you for your time and I will be looking forward to hearing from you in the very near future.*

**William J. Neil**
San Antonio, TX.

**Editor:**

*"Tactical Air Reconnaissance" (Jul-Sep 83) was of interest to me both as an RF-4 pilot, and as the 4441st Tactical Training Group (Blue Flag) recce staff officer. Two aspects of the article warrant comment: the discussion of U.S. Air Force aircrew proficiency, and the "United States Air Force Tac Recce Cycle" diagram.*

*Under-utilization of Air Force recce by Army requestors is not a significant factor in aircrew proficiency. Flying skills are largely determined by practice in the various mission types and events. The frequency at which they must be accomplished is based upon such factors as individual experience, crew position, and mission flying status. Accordingly, each major command specifies semi-annual sortie and event requirements in their flying regulations. Aircraft utilization rates (sorties per month per aircraft) also enter into the picture. Within Tactical Air Command, the RF-4 utilization rate has steadily increased over the past three years, thus providing recce units with more sorties. These factors all contribute to the development of unit operating budgets. More Army requests do not result in more flying hour dollars being added to a unit's budget, nor do they increase the numbers of sorties that will be flown.*

*As to the rarity of "truly skilled" recce pilots and navigators . . . Aircrews are certified Mission Ready (MR) after passing initial mission qualification check rides. These checks, which are in addition to yearly instrument proficiency flight evaluations, become annual requirments in order to maintain MR status. During these checks, all aspects of simulated combat missions are closely scrutinized by highly qualified flight examiners, who monitor the inflight portions from "chase" aircraft. Target acquisition and smart tactics against prebriefed threats are essential to passing mission qualification check rides. Just as individual aircrews receive annual checks, units are periodically evaluated through ORIs, tac evals, and other recurring higher headquarters and locally generated exercises. In my opinion, recce aircrews* **are** *truly skilled—as both individuals, and as flying units, they are frequently afforded the opportunity to prove it.*

*The "United States Air Force Tac Recce Cycle" schematic in this article is misleading. Judging from the title, it purports to be a generic U.S. system.*

*However, there are no ATOC's in the U.S. Tactical Air Control System—we have Tactical Air Control Centers (TACCs). ATOCs are found only in NATO's Central Region, and are not the same as TACCs. Regardless of which system is being illustrated, the diagram omits echelons above division, which are important in developing Army-Air Force apportionment, as well as preplanned mission requirements. Air support operations centers (ASOCs) are also omitted. They are the agencies through which immediate requests from corps and below are channeled to the TACC. In short, this diagram is erroneously titled and protrays a false picture of how Tac Recce is managed.*

*In spite of my previous comments, I do agree with the author's recommendation for Army units to request more recce. If we expect the "system" to work in wartime, we must exercise and train in it during peacetime.*

**Maj. Randall L. Atkinson,**
United States Air Force

**Editor:**

*The subject article, appearing in your Jan—Mar 83 edition of* ***Military Intelligence*** *intrigues me because I can't understand why the Center and School prefers the term "MI" or "CEWI" To say that "MI is . . . broad enough to include things as intelligence, signals intelligence, and electronic warfare" seems to stretch the conventional definition of "MI". CEWI (let's not overlook the EW aspect) has done a lot for the perceptions of what MI can do for the tactical commander in the past few years. Why tell us that we can have MI battalions (CEWI), but we can't say CEWI battalion? CEWI connotes the G2* ***and*** *G3 areas which are supported.*

*Although the Army doesn't operate on opinion polls, I suggest* ***Military Intelligence*** *magazine conduct a survey to ask the readers what they think about MI versus CEWI? The data obtained from such a survey might be of interest and value to the "doctrine writers." Major corporations spend huge sums of money to develop recognizable names (i.e., Exxon). Are we throwing away a name "CEWI", which has become recognizable in a positive way to the division/corps commanders and staffs?*

*Incidentally most officers and senior NCO's in my unit agree with Mr. Fauk. I'll have to work to change their minds on this issue.*

*In response to the superbly written article* **The Divisional CEWI Battalion: A Case for Reorganization,** *I would like to offer the following perspective. I, too, have previously advocated organizing the CEWI battalion into "brigade support companies", but now realize the present H Series T.O.E. organization works well. To the logical thinker, there is an instant attraction to the position "Organize CEWI symmetrically like everyone else is organized, i.e., into brigade support companies." Upon further examination and experience I've realized the current concept provides the following advantages: a. In peacetime: better training management. One company with all C&J assets or all GSR assets can structure a better training program than three companies—each with some C&J assets and some GSR assets. b. In wartime: a fulltime brigade IEW element provides a continuous staff relationship at the brigade TOC to work with the S-2 and S-3. Such an arrangement is not feasible if the company commander also has to task organize brigade support "packages" by having C&J or GSR platoons and other assets not tied to a particular brigade support company role—although under the present concept we do seek to develop habitual support relationships. c. Under the current CEWI concept the CEWI battalion "supports" the G2/G3 with the DTOC support element. The CEWI commander trains and resources the DTOC support element. Although a logical case can be made for putting this element into the division HHC, a logical argument also exists for not doing so: the present system works well—at least in the Second Armored Division. d. Locating the brigade support company commander in the brigade area does* ***not*** *necessarily make "communications better because distances are decreased." The critical distances are those distances between the forward C&J element and the TCAC—not the company commander and the C&J platoons. The commander with his small "CP" can always locate forward of the CEWI battalion headquarters when necessary. GSR's are normally with maneuver units. e. We can't bring too much of our CEWI C-E maintenance effort forward unless we duplicate expensive test and diagnostic equipment and PLL. Therefore resourcing the brigade support company with an adequate capability would probably require* ***more*** *33S personnel, more diagnostic equipment, and more PLL than is realistically available.*

*The present CEWI (H or J series) M.T.O.E. obviously is not perfect. There are many changes necessary regarding such basic issues as transportability, communications and maintenance. However, the drastic changes proposed in the article written by Major Paluska are not required in my judgement. While folks like me think about writing articles, folks like Major Paluska* ***do it.*** *He should be commended for a well thought out presentation. I just happen to see the issues from a different perspective.*

**Maj. John D. Skelton**
S-3, 522d MI Battalion (CEWI)
2d Armored Division

**Editor:**

*Your October-December 1983 edition of the* ***Military Intelligence*** *magazine contained an article on the QUICKFIX system written by Lt. Col. Michael N. McCloy where, in his prefacing paragraphs, he espoused a popular myth concerning the genesis of the system. The origination of QUICKFIX was quite different and for reasons that have yet to be accomplished.*

*QUICKFIX was developed in response to a Qualitative Material Requirement (QMR) written at Headquarters USAREUR in 1969. The bottom line capability was for QUICKFIX to locate tactical surface-to-surface missile units, in near realtime, with sufficient accuracy to bring firepower to bear. To obtain this capability, the then CINCUSAREUR had agreed to trade-off a critically needed helicopter lift company to provide the necessary platforms. Included in the capability requirement list was the specification for a 25 watt jammer, the sole purpose for which was to qualify the system for electronic warfare funding as intelligence system funding was simply unobtainable.*

*The QUICKFIX bottom line was not achievable using existing technology, a fact that was obscured and subsequently forgotten during QUICKFIX' development. Critical specifications (such as an accurate DF antenna and an on-board computer for target data base maintenance, platform navigation error reduction, and computation of target location) were degraded or deleted during the process-though always with the assurance that the bottom line would be unaffected. It was to no one's surprise at Headquarters USAREUR that when the prototypes were tested the bottom line was nowhere to be found. QUICKFIX was firmly rejected by*

(continued on page 21)

# THE COUNTERINTELLIGENCE OPERATIONAL CONCEPT

**by Major Martin G. Kloster**

TRADOC has approved the CI Operational Concept submitted by USAICS. The concept, which will be published as TRADOC Pamphlet 525-XX, provides the basis for CI operations in the 1980s.

The counterintelligence concept identifies the need for military intelligence to counter the multidisciplined intelligence threat to U.S. Army operations in the 1980s.It is structured to support the AirLand Battle Doctrine and any operations from battalion to Department of Army level. The overall objectives of the concept are to establish the relationship between CI and intelligence support to operations security, rear area protection and deception; to develop a basic philosophy for CI operations; and to identify training and doctrine requirements.

The multidiscipline approach to CI stems from the need to counter the full spectrum of the hostile intelligence collection effort. It is designed to counter hostile human intelligence, signals intelligence and imagery intelligence threats. Based on this new approach, the definition of CI has expanded to include the following: *Counterintelligence: Those intelligence activities intended to detect, evaluate, counteract or prevent hostile intelligence collection, subversion, sabotage, international terrorism, or assassination conducted by or on behalf of any foreign power, organization, or person operating to the detriment of the U.S. Army. It includes the identification of the hostile multidisciplined intelligence collection threat, the determination of friendly vulnerabilities to that threat, and the recommendation and evaluation of security measures.* (TRADOC Pamphlet 525-XX, CI Operational Concept.)

The concept describes CI support to OPSEC and points out that while CI supports this area, it is not synonymous with OPSEC. Units receiv-

ing CI support have a major responsibility for OPSEC that includes developing and implementing their command's OPSEC program. In addition, CI supports rear area protection through identification, location, and neutralization of hostile troops, agents and saboteurs targeted against the rear area. Deception is also supported by CI. While deception can be recommended as an OPSEC countermeasure, it can also be supported by CI when used as a separate tactical operation to portray intended intelligence indicators.

The concept also identifies a requirement for CI analysis. This analysis brings together the counterdisciplines and provides an integrated product that supports commanders in their decision making process. To accomplish this analytical function, the concept addresses the functional split of the former OPSEC management and analysis section. Traditionally the G3 is the OPSEC manager for a commander, and the CI concept does not change this responsibility. The management function will be performed by personnel assigned to the OPSEC staff element under the G3. The analysis function will be performed by intelligence personnel in a CI analysis section under the G2. The concept does not eliminate any of the OPSEC M&A Section functions, but is does clarify responsibilities and redistributes personnel resources to ensure the G2 and G3 can accomplish their mission.

The CI concept views the hostile intelligence collection threat as multidisciplined, and provides information in several areas where guidance was lacking, such as rear area protection, deception, tactical agent operations and OPSEC process. As pointed out earlier, changes in training and doctrine will be required, and USAICS has already initiated several actions that will conform to the concept. These actions include a review of career management field 96; development of new programs of instruction for CI training, and the publication of FM 34-60, Counterintelligence Operations and FM 34-60(A), Counterintelligence Special Operations.

A review and subsequent restructuring of CMF 96 has been submitted by USAICS to the Soldier Support Center, U.S. Army Military Personnel Center. Two items included in this restructuring are the inclusion of signal security personnel in CMF 96, and the reinstatement of the 97B10 program. Several problems were identified in the intitial 97B10 program; however, these areas will be corrected under the new program. These corrections include, but are not limited to, establishing tables of organization and equipment and tables of distribution and allowances positions prior to recruiting; ensuring recruiters have the proper job description for 97B10; implementing the personnel security screening program during the recruiting process developing a POI specifically for 97B10s, and providing for a systematic return of 97B10s to USAICS for transition training following a unit assignment. In short, the initial 97B10 program was a good idea, but required additional staffing coordination. The revisions made will ensure that this program is a viable source of CI personnel.

The first coordinating draft of FM 34-60 was sent to the field in early September 1983. This FM will replace FM 30-17, and will incorporate the new CI concept philosophy. In addition, work has been started on FM 34-60(A) to replace FM 30-17(A) and will be sent to the field in the coordinating draft in fiscal year 1985.

Lastly, new programs of instruction for 97B20, 97B20-Transition and 97B10 training have been completed, with supporting lesson plans. The 97B20 POI has been approved by TRADOC, and will be implemented in May 1984. The 97B10 and 97B20-Transition POIs will be approved by the Training and Doctrine Command, and will be approved once TO&E and TDA positions for 97B10s have been identified. Several changes to the POIs have been made as a result of the concept. In addition, new methodologies have been incorporated that will increase the realism, hands-on training and the "how to" approach in the course of instruction. While not all inclusive, the following examples illustrate changes that have been made in the POIs:

- Personnel security investigations will no longer be taught as the primary CI investigative mission. U.S. Army CI investigations (SAEDA, walk-ins, etc.) will be used. PSI will be taught, but only as it applies to the Army's mission in support of the Defense Investigative Service.
- CI analysis will be taught, and analytical techniques will be required in several practical exercises throughout the course.
- Instruction on OPSEC, RAP and deception have been expanded, with emphasis on hands-on training and how CI supports these areas.

Several other actions have been initiated which will improve the quality of CI instruction. One such action involves placing the entire course of instruction into a scenario environment. The advantages of this approach include: increased realism, a higher degree of understanding of how CI supports the overall Army mission, and greater retention of skills taught at USAICS. The implementation date for this method of instruction is May 1984. This approach eliminates the previous "block of instruction" format where students were provided instruction but not required to apply the knowledge in a simulated field environment or required to retain the information beyond the subject examination.

In summary, the Intelligence Center and School is moving forward with training and doctrine developments based on the CI concept. Future issues of **Military Intelligence** will include further information on the role of CI in OPSEC, RAP, and the new POIs. ★

---

*Major Martin G. Kloster is currently assigned as the Deputy Director, Department of Human Intelligence, USAICS. He holds a B.S. from South Dakota State University and an M.S. from the Naval Postgraduate School, Monterey, CA. He graduated from South Dakota State University in 1971, and has since attended the Armor Officer Basic Course, the Conterintelligence Officer Course, the MI Officer Advanced Course and the Armed Force Staff College.*

# Intelligence and PSYOP in TERRORISM COUNTERACTION

by Capt. Michael McEwen

### Terrorism and Low Intensity Conflict

Terrorism counteraction is a mission that the Army can expect to face in the 1980s and 1990s, especially if present policies on Foreign Internal Defense (FID) are continued. International trends indicate that insurgency will continue in several regions where the U.S. has national interests at stake. This probably means continuing Army involvement in low intensity conflict environments where terrorism is commonplace.

Low intensity conflict is defined as "guerrilla warfare, revolution, subversion or other tactics aimed at internal seizure of power."[1] Other officially defined levels of conflict are mid intensity, which is a full-scale conventional war between nations, but limited in global scope; and high intensity, which includes the use of nuclear, biological, and chemical weapons and/or multi-regional areas of conflict.[2] FID is the participation of U.S. military and civilian agencies in the efforts made by a host nation to free itself from subversion, insurgency, and lawlessness.[3]

The Army has many responsibilities in FID. Among these, several appear to have special importance in the general area of terrorism counteraction:

- Developing language-trained and area-oriented Army forces and personnel as necessary to train, advise or assist indigenous forces.
- Conducting research and development activities in support of internal defense and internal development to include psychological operations and civil affairs.
- Conducting intelligence and counterintelligence operations.
- Participating with other services in joint internal defense training and exercises as mutually agreed upon by the services concerned.

Of course, the particular plans and programs conducted by Army forces and personnel will be part of the larger plan developed by the U.S. country team under the direction of the ambassador or senior State Department representative. FM 100-20, Low Intensity Conflict, details the doctrine, policy, and coordination that control the activities of U.S. agencies involved in FID operations.

Army personnel will face a wide range of threats in the low intensity conflict environment, and terrorists will be present in most cases. Acts of terrorism usually require minimal support, compared to other operations and can have a great impact in advancing the insurgent cause. Unfortunately, FM 100-20 does not deal with the problem of terrorism counteraction except in a very limited manner. This manual is devoted primarily to the role of security and police organizations in reaction to terrorist activities, and offers relatively little guidance in terrorism assessment and counteraction planning.

A systematic analysis of terrorism ought to begin with the definition of key terms. The most obvious concept to define is terrorism. One widely used definition of terrorism has been employed in annual reports which are compiled and released by the Department of State and the Central Intelligence Agency:

"Terrorism is the threat or use of violence for political purposes by individuals or groups, whether acting for, or in opposition to, established governmental authority, when such actions are intended to shock, stun, or intimidate a target group wider than the immediate victims."[5]

This definition of terrorism points out two aspects of the phenomenon that distinguish it from other types of political violence (warfare). First, the primary purpose of the action is to "shock, stun, or intimidate." Second, it is important to stress that a terrorist's **target** is usually relatively small while his **target audience** is relatively large. Note that terrorism is psychological warfare, and target audience impact is its primary objective.

The variety of terrorism most widely publicized in the news media over the past decade is usually labeled "international terrorism," Scholars and other students of terrorism have sometimes tried to bring more precision to the study of terrorism by offering other terms such as transnational terrorism and non-territorial terrorism which were defined in a manner that allowed them to be distinguished from the more general category. These special terms have utility in their intended application, but they are probably not necessary in examining the Army's role in FID. The commonly used U.S. government definition of international terrorism is "terrorism conducted with the support of a foreign government or organization and/or directed against foreign nationals, institutions, or governments."[6] This definition is obviously very broad. It requires only that the target and terrorist be "foreign" to each other. Under this definition almost any terrorism taking place in a country where the U.S. is conducting FID operations could be called international terrorism because of actual or potential involvement of U.S. personnel or facilities as targets of the insurrection.

Because this broad characterization of international terrorism might obscure certain important aspects of the overall picture, it is probably useful to distinguish terrorism in a given FID area of operations as *inter*national or *intra*national, on the basis of the primary target audience. It is important to recognize the special characteristics of this new term: intranational terrorism is directed primarily at a host nation target audience. It is intranational even though it may involve the United States or another foreign nation as the actual target for attack.

This distinction is important because certain aspects of the re-

sponse to terrorism should be determined by the primary target audience. Since terrorism is a form of psychological operations, it is very important to analyze the proper target audience in formulating responses. If the target audience is international, then major emphasis should not be directed at intranational audiences, and vice versa. Although tactical and direct counteraction measures will be focused on the terrorist group, the greater counteraction task is to determine an appropriate psychological counter effort that can be directed at the target audience. Army personnel involved in FID operations should be aware of this distinction.

Another bit of terminology is becoming increasingly important within the Army's sphere of terrorism studies and operations. There are now three terms which are coming into standard use to describe the specific types of activity. **Terrorism counteraction** is the generic term that is intended to encompass the overall field. **Antiterrorism** is the term for the preventive and preemptive side of terrorism counteraction, while **counterterrorism** is being used to indicate the active measures taken in direct response to specific and often on-going terrorism incidents. To put it another way, antiterrorism is preventive medicine and counterterrorism is immediate emergency treatment. The distinction between the two terms may be difficult to discern in realworld situations, but the differences are important to understand. Much of the activity in Army terrorism counteraction has been in the counterterrorism field because that is a natural direction for a combat-oriented organization. However, in many situations, especially operations such as FID in an insurgency environment, antiterrorism may be the more important activity to emphasize.

**Terrorism counteraction planning**

The particular terrorism counteraction required in any given FID situation will clearly depend on the level and nature of the terrorism activity. The guidance in FM 100-20 emphasizes maximum use of intelligence assets and close cooperation with host nation law enforcement agencies. These are sound principles and have a definite place in terrorism counteraction. Using these ideas and the additional concepts introduced in the preceding discussion, it is possible to outline a basic approach for planning and operations.

The best possible intelligence is necessary to deal effectively with terrorism because a terrorism campaign can be carried out by a small and relatively independent group of operators. This makes the collection phase of the intelligence cycle very difficult. Because of their familiarity with the local situation, the host nation's law enforcement agencies are the primary intelligence resource. Guidance in FM 100-20 stresses that the host government "must emphasize intelligence and police operations to counter clandestine organizational, intelligence, logistic, and terrorist activities."[7] The host nation police may have excellent intelligence resources, but these may fall within the traditional boundaries of police work. The effective use of intelligence in terrorism counteraction must include activity in other areas.

In an excellent article on terrorism and intelligence, Schlomo Gazit and Michael Handel discuss the categories of information which can be gathered on terrorist groups.[8] In reviewing these, it becomes clear that traditional criminal investigation and intelligence may not be sufficient to yield the maximum possible useful information. Gazit and Handel describe the need for intelligence on:

The ideological and political system—understanding the ideological base and how it functions will give important clues that may point to vulnerabilities and susceptibilities;

The organizational/operational infrastructure—it is obviously important to understand the organizational system, mechanism and resources which allow a terrorist group to operate;

The operational activities of the organization—these are the clear and immediate hazards posed by a terrorist group, and it is vital to obtain the maximum possible advance indications or warnings of specific terrorist operations and to identify targets for counteraction;

The support infrastructure—this element is distinguished from the organizational/operational infrastructure because it is comprised of the civilian support base, and undermining this base could cripple a terrorist group;

The international connections—for many terrorist groups, aid and assistance received from outside sources is absolutely necessary, and intelligence on this aid is definitely important.

It seems clear that the scale of the intelligence operation necessary to cover these targets is probably beyond the normal limits of intelligence activities of most law enforcement agencies. Army FID personnel should endeavor to help build intelligence assets that are equal to the task outlined if successful terrorism counteraction campaigns are to be achieved. Certain limits may have to be recognized however. U.S. law and policy limits the types of intelligence activity that can be conducted, and some of the deep penetration that would be required to cover the intelligence arena adequately might be outside U.S. guidelines. In such cases, the host nation's personnel may have access to the required intelligence assets and may provide information that is sorely needed by FID personnel. When intelligence requirements are being serviced to the best possible degree, the terrorism counteraction analysts and planners can begin to focus on anti and counterterrorism activities. It is obvious that a number of variables relating to the threat and the counteraction assets will determine the exact nature of specific programs. In a general sense, it is possible to list some of the basic techniques that might be employed.

In counterterrorism, FID assistance provided by the Army could be directed at improving tactical response capabilities by host nation armed forces and law enforcement (although certain kinds of assistance to police agencies by U.S. armed forces are prohibited). Assistance provided by Army Mobile Training Teams and other assets could include training in small unit assault tactics (including urban terrain tactics),explosive ordnance disposal, riot control, emergency medical care, and surveillance methods. Efforts should be made to train effective counterterrorism teams in all regions of the host nation in order to develop a widespread deterrant to terrorist activity.

The antiterrorism assistance provided should include comprehensive security training including installation/facility security, personal protective measures, operational security,

and counterintelligence. Plans should also be made to assist the host nation in training personnel for penetration of terrorist and support organizations in order to increase the effectiveness of intelligence efforts. The agents may also be able to generate disruptions in groups they penetrate. And last, but far from least, the antiterrorism campaign should include a counterpropaganda program. Since terrorism is a form of psychological warfare, it should be countered with appropriate activity. Accurate target audience analysis and effective PSYOP campaigns can neutralize the impact of terrorism. Creative and effective PSYOP may be the ultimate weapon because terrorism cannot exist if the target audience is immunized against its impact. This goal may be difficult or even impossible to fully achieve, but any progress towards it will diminish the effectiveness of terrorism, perhaps even to the point where the level of activity is significantly reduced.

**PSYOP targets and techniques**

The basic doctrine of Army PSYOP is described in FM 33-1, Psychological Operations. Chapter 5 of that manual, "PSYOP In Support of Foreign Internal Defense," discusses the aspects of PSYOP that are likely to be used in antiterrorism activities, even though the manual does not directly address terrorism at length. Three basic categories are used to plan and structure such campaigns: PSYOP targets of opportunity, traditional PSYOP campaigns, and deception operations.

The target of opportunity efforts would be based on the successful results of the host nation and U.S. counterterrorism efforts. Whether these are law enforcement activities, conventional counterguerrilla military operations, or covert actions, they should be fully exploited by appropriate propaganda campaigns designed to emphasize the host nation's ability to deal with and eliminate terrorism. Coordination between PSYOP personnel and the counterterrorism forces would obviously provide lead-time which could increase the prospects for success. Even if such prior planning is not possible, PSYOP planners should always be alert for targets of opportunity.

Traditional PSYOP campaigns can address many of the vulnerabilities of terrorist organizations. The insurgents themselves can be attacked with programs designed to create uncertainty and dissention. Examples are rumors of spies and informers, allegations of special treatment of officers and/or leaders, and amnesty/incentive programs for terrorists who surrender. Skilled PSYOP planners with access to good intelligence may also be able to develop special programs aimed at the terrorist leadership which could exploit rivalries between competing leaders and groups. The general populace, both supportive and nonsupportive of the terrorists, should be subject to substantial campaigns. Opinion leaders in these groups could be given special briefings and selected intelligence data to support the government's position (the news media and religious leaders are especially important segments to remember in these efforts). The PSYOP should always stress the inhumanity and immorality of the terrorist activities while emphasizing that the actual impact (deaths, injuries, and property losses) is relatively small.

The implementation of effective deception operations could have great impact on terrorist groups. Planned leaks of false government plans, planting or loss of false documents, use of double agents, and radio transmission of deception messages all contribute to confusion, inefficiency, and decreased operational capability of terrorist forces.

It should be obvious that the Army forces committed in a given FID situation may need special personnel resources in order to conduct effective PSYOP assistance to the host nation. Mobile Training Teams can be developed and deployed as needed to handle training requirements, but the Army and Country Team leadership may need additional staff resources in order to adequately evaluate the situation and develop PSYOP assistance plans. Minimal staff augmentation probably ought to include officers with PSYOP, military intelligence, and Special Forces skills. Such a range of expertise will provide the analytical tools needed to address the full range of antiterrorism PSYOP discussed above.

Low intensity conflict situations, especially FID operations, put Army personnel in high-threat terorrism environments. Since terrorism is a type of psychological warfare, Army FID organizations should be prepared to deal with that aspect of the problem as well as the direct physical threat to specific targets. A balanced program of counter and antiterrorism assistance to the host nation should create forces with the capability to neutralize present threats while preempting future ones. The vigorous and extensive use of PSYOP can dramatically enhance antiterrorism programs. ★

**Footnotes**

1. FM 100-20, Low Intensity Conflict, p. 14.
2. IBID.
3. IBID.
4. IBID., pp. 125-126.
5. "Patterns of International Terrorism: 1981", U.S. Department of State, July 1982, p. i.
6. IBID.
7. FM 100-20, p. 29.
8. Gazit, Schmolo and Michael Handel, "Insurgency, Terrorism and Intelligence," in Intelligence Requirements for the 1980s: Counterintelligence, Roy Godson, ed., National Defense University, 1980, pp. 131-135.
9. FM 100-20, p. 213.

---

*Captain Michael T. McEwen is an instructor in the Department of Psychological Operations, School of International Studies, at the John F. Kennedy Special Warfare Center, Fort Bragg, NC. He was commissioned in the Oklahoma Army National Guard upon graduation from Officer Candidate School and served in several assignments in the Oklahoma Guard before being called to the Active Army in 1982. He has completed the Infantry Officer basic and advanced courses, the Psychological Operations Officer Course and the Military Intelligence Officer Branch Qualification Course (Advanced). His civilian education includes a master's degree from the University of Oklahoma where he specialized in international terrorism studies.*

**SUBSCRIPTION ORDER FORM**

Deposit Account Number

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | – | | |

*Enclosed find $_____ (check or money order), or charge to my Superintendent of Documents Deposit Account Number shown above.*

*Your Order Number_____*

*Please send the subscription(s) I have listed to the address shown at the bottom of this form.*

MAIL ORDER FORM TO:
Superintendent of Documents
U.S. Government Printing Office
Washington, D.C. 20402

| FOR OFFICE USE ONLY | |
|---|---|
| Quantity | Charges |
| ------ Enclosed | |
| ------ To be mailed | |
| ------ Subscriptions | |
| Postage | |
| Foreign handling | |
| MMOB | |
| OPNR | |
| ------ UPNS | |
| ------ Discount | |
| ------ Refund | |

master charge

VISA

Credit Card Orders Only
Total charges $_____. Fill in the boxes below:

Credit Card No.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | |

Expiration Date Month/Year

| | | | |
|---|---|---|---|
| | | | |

Master Charge Interbank No.

| | | | |
|---|---|---|---|
| | | | |

*NOTE: Complete top address portion if different from that at the bottom.*

Name_____

Street address_____

City and State_____ ZIP Code_____

| SYMBOL | TITLE | PRICE |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

NAME—FIRST, LAST

COMPANY NAME OR ADDITIONAL ADDRESS LINE

STREET ADDRESS

CITY | STATE | ZIP CODE

(or) COUNTRY

PLEASE PRINT

GPO Form 3625
(3-79)

## ORDERING INFORMATION

The prices of all U.S. Government publications sold by the Superintendent of Documents are established by the Public Printer in accordance with Title 44 of the United States Code. Prices are subject to change and the prices charged on your order will be those in effect at the time your order is processed. As it is not feasible to manually correct the prices in the publications affected by price changes, the prices charged on your order may differ from those printed in the publications. Although the issuing agencies generally know about price changes, some agencies inadvertently continue to publish announcements, order forms, and catalogs which contain erroneous prices. Frequently, the news media publishes articles with erroneous or outdated prices.

---

Subscriptions are accepted for 1 year only unless otherwise specified. Subscribers will be notified prior to the expiration of their subscription in ample time to effect a continuity of service.

---

Orders to foreign countries require a special handling charge. The charge is approximately one-fourth of the current selling price of the subscription service ordered and is included in the Foreign subscriptions price. This charge is to cover the special handling required to comply with the customs and international mailing regulations.

---

The average processing time for new subscriptions takes 2 to 6 weeks plus mailing time. The large volume of mail we receive each day makes it virtually impossible to locate a subscription order until it has been entered into our computer. Please take this into consideration before making inquiry concerning periodicals and subscription services in compliance with Paragraph 1708 of Title 44, U.S. Code. Effective January 1, 1974, for orders entered or services commencing after that date, the discount policy is:

A discount of 25 percent will be allowed to bookdealers when the publications, pamphlets, periodicals or subscription services are mailed, delivered or forwarded to the dealer's normal place of business.

A discount of 25 percent will be allowed to quantity purchasers (100 or more copies of a single publication, pamphlet, periodical or subscription service) when mailed to a single address.

No discounts will be allowed when the publication, pamphlet, periodical, or subscription service is mailed to a third party (unless in quantities of 100 or more), or on those periodicals or subscription services which fall into a special pricing category.

### WHERE TO ORDER

Orders should be addressed to the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. In addition to your address, please include the title and price of the subscription together with the subscription symbol that appears in the brackets following the price. For example: **[COBD]** identifies the Commerce Business Daily.

### HOW TO REMIT

The rules of this Office require that remittance be made in advance of shipment of your subscription. Your check or money order should be made payable to the Superintendent of Documents. Foreign money and postage stamps are not acceptable. Remittances from foreign countries should be made by international money order payable to the Superintendent or by draft on an American or Canadian bank. UNESCO Coupons are also acceptable from foreign countries. For the convenience of customers who make frequent purchases, a prepaid Deposit Account may be opened by remitting $50 or more. Upon receipt in this Office,you will be assigned a special Deposit Account Number against which future orders may be placed without making individual remittances or first obtaining quotations. It is suggested that a balance sufficient to cover 3 months' purchases be maintained to avoid the necessity of frequent deposits. Orders may also be charged to your Master Charge or VISA account. Please include your card number, date of expiration, and interbank number *(Master Charge only).*

GPO: O 293-641

# THE HAVERSACK RUSE

by Capt. Harold E. Raugh

Since the days of the Trojan horse, military deception and ruse have been effective instruments when used by an innovative commander to deceive and defeat an enemy, minimizing friendly casualties and the expenditure of valuable resources in the process.

One of the most effective strategems in military history occurred during the Palestine Campaign of World War I. This campaign had been characterized by mediocrity and lack of ingenuity on the part of the senior British commanders, until the appointment on 28 June 1917 of General Sir Edmund H.H. Allenby as Commander-in-Chief, Egyptian Expeditionary Force.

Soon after General Allenby's arrival, preparations were finalized for the Third Battle of Gaza, after the first two battles (conducted in January 1917 and April 1917) had ended in dismal failure for the attacking British. This was the fourth year of the war, and all hope of ending the war in 1917 was gone, due to the collapse of the Russians, demoralizing failure of the French offensive in Champagne, and lackluster results of the Allied spring offensive. A decisive victory was needed to sustain the morale and confidence of the British people. Prior to departing for Egypt, British Prime Minister David Lloyd George confirmed that belief by telling General Allenby that "he wanted Jerusalem as a Christmas present for the British nation."[1] The Prime Minister's firm conviction was reinforced in a telegram sent to General Allenby in August 1917, admonishing the general to continue pressuring the Turks "to strengthen the staying power and morale in this country."[2]

With these strong admonitions in mind, General Allenby's plan (a slightly modified version of a plan developed by Lieutenant-General Sir Phillip Chetwode, Commander of the "Eastern Force" prior to General Allenby's arrival) was to sieze Gaza without making the same costly and unsuccessful frontal assaults against strong defensive positions as had been done in the first two battles. The course of action decided upon was to initiate a feint against Gaza, consisting of a limited infantry attack and systematic artillery bombardment. Shortly thereafter, two cavalry and three infantry divisions were to capture Beersheba on the enemy's left flank, and seize its all-important water wells. Then the infantry would roll up the enemy's defenses and capture Gaza from the left flank, while the cavalry moved to intercept and destroy the withdrawing Turks.[3] (See diagram, "Third Battle of Gaza.") This attack on the enemy's left flank would need to be timed perfectly, to coincide with the Turks sending their reserve troops from Gaza to Beersheba.[4]

Preparations taken to deceive the enemy were numerous, but possibly the most effective has since come to be known as "the haversack ruse." Conceived by Colonel Richard Meinertzhagen[5], head of Military Intelligence at General Headquarters, Egyptian Expeditionary Force, this plan was enthusiastically sanctioned by General Allenby in September 1917. The scheme was that a staff officer, ostensibly on a reconnaissance mission, would contrive to be chased by Turkish outposts, pretend to be wounded, and would drop his haversack, freshly stained with his horse's blood. This was intended to deceive the enemy that the main attack would be coming at Gaza. The portfolio was ingeniously compiled to look as real as possible[6], and contained:

- a staff officer's estimate of the situation, complaining about the command's obstinacy in attacking at Gaza instead of at Beersheba;[7]
- a report in the staff officer's notebook disclosing the inability of the British commander to overcome the water shortage and transport difficulties in maintaining a large force before Beersheba;[8]
- a large number of pound banknotes, in a sum large enough to give the impression that they wouldn't have been "lost" on purpose;
- an agenda for a meeting at Allenby's headquarters;
- rough notes about a cipher;
- a telegram announcing a reconnaissance around Beersheba;
- orders for an attack on Gaza;
- a map with arrows pointing at Gaza;
- a number of personal letters, including one announcing the birth of a son to a staff officer. Written by Colonel Meinertzhagen's sister Mary, this letter concluded: "Good-bye, my darling! Nurse says I must not tire myself by writing too much, so no more now but I will write again soon and then it will be a longer letter than this. Take care of your precious self! All my love and many kisses. Your loving wife, Mary. Baby sends a kiss to Daddy!"[9]

Two unsuccessful attempts were made to "deliver" the falsified information to the Turks, so Colonel Meinertzhagen himself took the haversack on the third try, and on 10 October 1917 he rode towards Beersheba. His diary notation best relates this episode:

> I was well mounted, and near Girheir when I found a Turkish patrol who at once gave me a chase. I galloped away for a mile or so and then they pulled up, so I stopped, dismounted, and had a shot at them at about 600 yards. That was too much for them, and they at once resumed the chase, blazing away harmlessly all the time. Now was my chance, and in my effort to mount I loosened my haversack, field glasses, waterbottle, dropped my rifle—previously stained with some fresh blood from my horse—and, in fact, did everything to make them believe I was hit and that my flight was disorderly. They had now approached close enough, and I made off, dropping the haversack which contained the notebook and various maps, my lunch, etc. I saw one of them stop and pick up the haversack and rifle, so I now went like the wind for home and soon gave them the slip, well satisfied with what I had done and that my deception had been successful.[10]

The haversack was processed through Turkish command channels, with the captured intelligence data ultimately reaching the German

**Phase I: Deployment** *(October 24-30)*

The Twentieth Corps moved east towards Beersheba, the Twenty-first Corps remaining opposite Gaza. The Twentieth Corps had practically the whole of the transport of the army, the Twenty-first Corps being left immobile. One mounted division covered the gap between the two corps. The remainder of the Desert Mounted Corps moved south to Khelasa and Asluj. From October 27 the Twenty-first Corps, assisted by warships, carried out a heavy bombardment of Gaza.

**Phase II: Capture of Beersheba** *(October 31)*

The Twentieth Corps captured the main defences of Beersheba while the mounted troops, after a night march of thirty miles, attacked the town from the north-east. The Twenty-first Corps continued the bombardment of Gaza.

**Phase III: Attack on Gaza** *(night of November 1-2)*

While the Twentieth Corps was preparing to attack the left of the Turkish main line the Twenty-first Corps assaulted a portion of the Gaza defences in order to attract the enemy reserves. Meanwhile the flank-guard of the Twentieth Corps became heavily engaged in the hills north of Beersheba, at Khuweilfe.

**Phase IV: Exploitation as intended by G.H.Q.**

While the Twentieth Corps broke the Turkish left, the Desert Mounted Corps was to pass round this flank and intercept the retreat of the whole Turkish army.

**Phase IV: Exploitation as it actually occurred** *(November 6)*

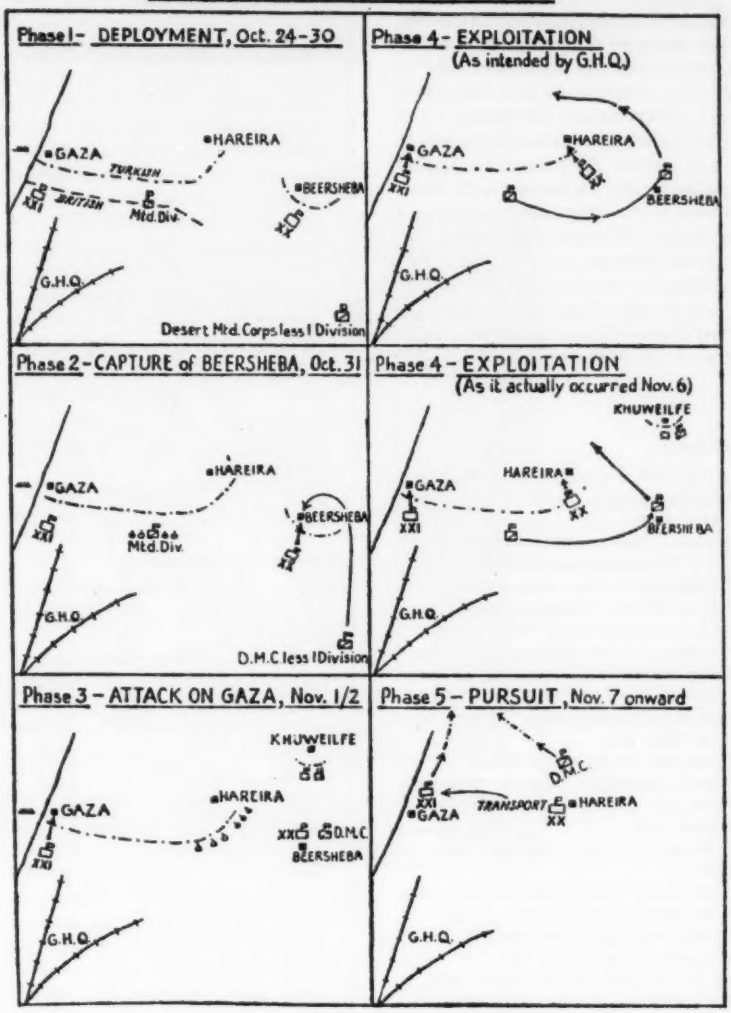
Owing to the fighting at Khuweilfe and the water difficulties, the mounted troops were scattered and tired, instead of collected and fresh, when the moment came. As the Turks still held out at Khuweilfe the mounted troops had to pass through a comparatively narrow gap, instead of round a flank. Only four brigades of ten were immediately available.

**Phase V: Pursuit** *(November 7 onward)*

Owing to the supply and water problem, the Twentieth Corps had to halt after November 6 and transfer all its transport to the Twenty-first Corps, who took up the pursuit along the Plain of Philistia.

**From Wavell, Allenby, pp. 214-215.**

## THIRD BATTLE OF GAZA




commander of the Turkish forces, General Kress von Kressenstein.

This simple ploy, coupled with all of the other British deceptions, convinced General von Kressenstein that the main British assault would be against Gaza. Even though he realized the possibility that the documents may have been fake, General von Kressenstein felt obliged to act as if they were genuine, as he could not conceive of an attack being made in any direction other than directly at Gaza.[11]

When the Third Battle of Gaza commenced on 31 October 1917, enemy dispositions revealed that they had in fact been deceived as to the British plan of attack. After a week's hard fighting with heavy losses, the Turks abandoned the Gaza-Beersheba line which they had held for the previous nine months. They were in full retreat to the north, and the British were able to fully exploit this success. Only five weeks after the capture of Gaza on 11 December 1917, General Allenby formally entered the captured city of Jerusalem. He had provided the British Prime Minister with his desired Christmas gift.

The intricately planned, audaciously executed, yet relatively simple "haversack ruse" directly resulted in the breaking of the stalemate at Gaza and the eventual British capture of Jerusalem. From 31 October 1917 to 11 December 1917, 12,000 Turkish prisoners and 100 artillery pieces were

taken. Turkish casualties were 25,000 as compared to 18,000 for the British.[12]

Throughout history, military forces and commanders have been deceived, and defeated by the employment of clever ruses. The "haversack ruse" is but one example of such deception and contemporary commanders and intelligence officers would do well to study other historical deception methods, and implement such stratagems in training exercises. Military professionals should endeavor, as did General Allenby (in the words of T.E. Lawrence, "Lawrence of Arabia"), to "turn the use of deception from witty hors d'oeuvres before a battle into the main point of strategy."[13] ★

**Footnotes**

1. Colonel A.P. Wavell, C.M.C., **The Palestine Campaigns.** (London: Constable, 1931), p. 96.
2. Wavell, **The Palestine Campaigns,** p. 96.
3. Cyril Falls, **Armageddon 1918.** (London: Weidenfeld and Nicholson, 1964), p. 28.
4 Brian Gardner, **Allenby of Arabia.** (New York: Coward-McCann, 1965), p. 125.
5. Falls, p. 55, and Gardner, p, 128, listed Meinertzhagen's rank as "Colonel", whereas it is listed as "Major" in J. Barton Bowyer's **Cheating.** (New York: St. Martin's, 1982), p. 81.
6. General Sir Archibald Wavell, K.C.B., C.M.G., **Allenby: A Study in Greatness.** (New York: Oxford, 1941), p. 202.
7. Falls, p. 55.
8. Wavell, **The Palestine Campaigns,** p. 106.
9. John Lord, **Duty, Honor, Empire.** (New York: Random House, 1970), p. 332.
10. Meinertzhagen Diary entry, 10. 10. 17, as quoted in Gardner, p. 130.
11. Lt. Col. Clive Garsia, D.S.O., M.C., **A Key to Victory.** (London: Eyre and Spottiswoode, 1940), p. 209.
12. Wavell, **The Palestine Campaigns,** p. 167.
13. Bowyer, p. 81.

# MI Writer's Guide

**Military Intelligence** is oriented toward active Army, reserve and civilian intelligence personnel throughout the Army and Defense intelligence communities. While writing an article, consider the readers. They range from privates to general officers to civilians, and they all have one thing in common: they work in, or have an interest in, military intelligence.

**SUBJECTS.** We are interested in all subjects relating to the diverse fields of military intelligence including Army doctrine and policies relating to intelligence; tactical and strategic intelligence; organization, weapons and equipment; foreign forces; electronic warfare; and intelligence collection (SIGINT, HUMINT, IMINT, etc.). Historical articles should have contemporary value. If you have an idea for an article, contact us and explain your theme, scope and organization. It will save both of us time and will facilitate our planning.

**STYLE. Military Intelligence** prefers concise and direct wording in the active voice. Every article should have a beginning that catches the readers' attention, a body containing the crux of the article, and an ending which concludes or summarizes. Keep the article as simple as possible. Avoid unfamiliar terms, unexplained abbreviations, and poorly constructed sentences. Don't submit a manuscript unless you are completely satisfied with it. Read it over three or four times and then let a friend read it. It is not uncommon to revise an article several times before submitting a finished manuscript. Don't waste the readers' time with meaningless or repetitive phrases and words. We edit all articles. However, a polished article is more likely to be accepted than a hurried mistake-riddled effort. Save yourself time and effort; be your own editor. We do not normally allow writers to review how their articles have been edited.

**ACCEPTANCE.** We make no prior commitments on acceptance until we have thoroughly studied each manuscript. All manuscripts must be original, previously unpublished works. Authors submitting articles are responsible for informing the staff of **Military Intelligence** of simultaneous submission and/or acceptance by other publications.

**FORMAT.** We prefer articles from 1,000 to 2,500 words in length. We will publish shorter or longer articles depending on quality. Develop your ideas and stop. Send clean, double-spaced manuscripts typed on one side of the sheet. Your name, length of manuscript, address, and phone number (Autovon preferred) should be typed on the first page. We prefer one original and one copy. Cite your references and enclose all quoted material in quotation marks. If possible, credit should be given within the article as footnotes are burdensome and use valuable space.

**GRAPHICS.** Artwork in the form of black and white glossy photographs, maps, sketches or line drawings can enhance the attractiveness and effectiveness of your article. If you have an idea for artwork or know of where we can get it, let us know.

**CLEARANCE.** The Office, Chief of Public Affairs, Department of the Army must clear certain categories of articles written by U.S. military personnel on active duty or by civilian employees of the Defense Department. Your local information officer can assist you on this.

**BIOGRAPHY.** Enclose a brief biographical sketch, including important positions and assignments, experience or education which establishes your knowledge of the subject, and your current position and title. Photos of authors are no longer used by **Military Intelligence.**

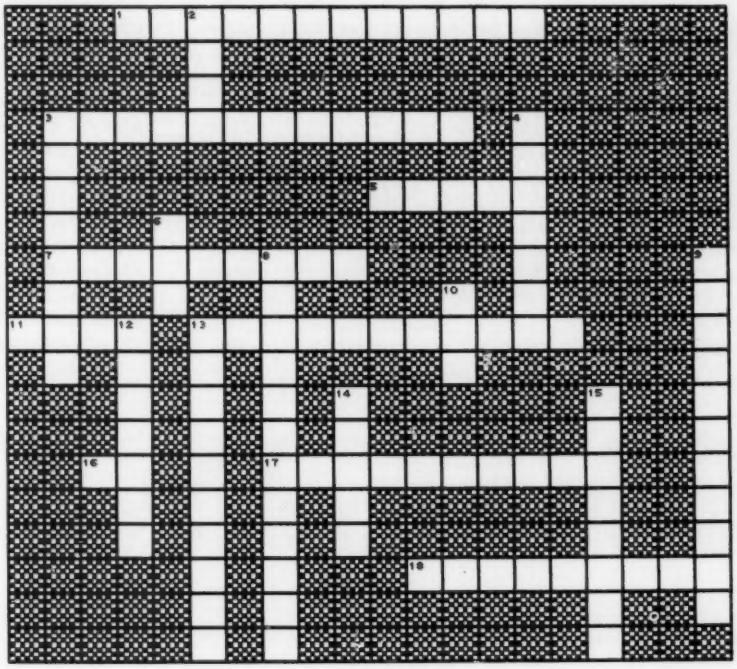
**COPYRIGHT. Military Intelligence** is not copyrighted. Acceptance by **Military Intelligence** conveys the right for subsequent reproduction and use of published material for training purposes.

**SUMMARY.** If you are interested in a subject, chances are that others will be too. Pick a subject, thoroughly research it, and think all your ideas through. Write with enthusiasm, but be natural. Don't adopt a different style.

FOR MORE INFORMATION, contact the Editor, Commander, USAICS, ATTN: ATSI-TD-MIM, Fort Huachuca, Ariz. 85613; or call Autovon 879-3033/3605, commercial (602) 538-3033/3605.

# Crossword Puzzle

COUNTERINTELLIGENCE



ACROSS CLUES

1. "HOME OF INTELLIGENCE"
3. TO CLOSELY WATCH,OVERSIGHT
5. DENY DISCLOSURE OF FRIENDLY ACTIVITIES
7. SYSTEMATIC USE OF COERCION
11. A WILY SUBTERFUGE
13. TO QUESTION SYSTEMATICALLY
16. DENIAL OF ENEMY INTELLIGENCE GATHERING (ACRONYM)
17. TO PERMEATE SOMETHING BY PENETRATION
18. THE PRACTICE OF SPYING

DOWN CLUES

2. A WILY SUBTERFUGE
3. ONE COMMITTED TO ACTIONS OF DESTRUCTION
4. ENCIPHER
6. USSR MAIN INTELLIGENCE DIRECTORATE (ACRONYM)
8. MENTAL ACUTENESS,SHREWDNESS
9. TO ENGAGE IN RECONNAISSANCE
10. COMMUNIST INTELLIGENCE AGENCY
12. A MEANS OF ELUDING
13. REBELLION AGAINST ONE'S ORGANIZATION
14. ENEMY,OPPOSITION (ACRONYM)
15. SOVIET SPECIAL PURPOSE UNIT



(solution on page 48)

*When the commanders of rear area protection operations survey the battle area and organize their assets to accomplish the mission, they must know that counterintelligence is a prime contributor to countering the third dimension.*

# COUNTERING the T

**by Maj. Richard Armstrong**

A tremendous amount of study is being done on the nuclear and conventional dimensions of future wars, but very little attention is being focused on an important third dimension—that of the unconventional forces and their potential impact on rear area security. As modern warfare moved from the exclusive domain of professional armies in previous centuries to a broad spectrum of military and paramilitary operations conducted in enemy held territory during the 20th century, the use of partisans, commandos, special forces and saboteurs has grown to supplement conventional ground force operations. This increased growth in the unconventional dimension to warfare creates a battle area not only along the front line of contending armies, but also in the rear areas of armies and in the homelands. The primary means of waging unconventional warfare against tactical operations is sabotage.

Sabotage is a relatively modern term that has its origins in the French word, sabot, a wooden shoe worn by the people of northern France and the Low countries. In the late 1800s, peasants employed in the textile industries of northern France organized into trade unions as a means of coping with management. They feared the loss of their jobs as hand weavers if factory owners continued to install textile weaving machines. Whenever they could do so unobserved, the workers would kick one of their wooden shoes, or sabots, into the moving parts of the machine to break or destroy these new machines. The French turned sabot into sabotage, which has since described the deliberate destruction of another's property. Modern military usage has broadened sabotage to include an act that obstructs a nation's war effort.

Despite the fact that sabotage is not new, there is very little known about it as far as the ordinary soldier is concerned. This unfamiliarity is understandable when the necessity

for security on the part of nations and individuals is taken into consideration. This silence creates a lack of information and contributes to a doctrinal void by U.S. forces about a dimension of Soviet military doctrine that devotes an enormous amount of attention to operations behind enemy lines. Soviet military doctrine sets forth a concept that seeks to attack simultaneously the entire depth of an enemy force's disposition, to include the homeland. In a coordinated effort, attacks in our rear areas will undermine our defense and facilitate the rapid advance of Soviet conventional ground forces.

The intent of this article is to briefly survey the role and operations of Soviet military unconventional warfare capabilities which are used in operational and tactical level support to conventional ground forces, and to discuss the U.S. Army counterintelligence role and methods used to protect friendly tactical operations from this threat.

# THE THIRD DIMENSION

Based on a legacy of successful World War II partisan and agent activities in the German army rear areas, the Soviet military maintains a significant number of forces for unconventional warfare missions in support of front and subordinate field armies. Soviet unconventional warfare doctrine can be divided into three basic levels: strategic, operational and tactical. The difference between these levels is the scope of the missions, the type of forces allocated, and the level of command and control.

Strategic level unconventional warfare conducted in the homeland of the enemy is under the control of the Committee for State Security (Komitet Gosudarstvennoy Bezopasnostic or KGB). While not directly supporting fronts or field armies, UW forces at this level are deployed under the control of the Soviet Union's intelligence and security organ with the greater mission of reducing the enemy's ability and will to continue the war. The scope of their missions would include efforts to intimidate and demoralize the populace, create general chaos through disruption of public utilities and services, and sabotage the national war effort. An example of possible missions for the strategic level was identified by former KGB Captain Aleksei Myagov, who knew about the plans to cause an outbreak of cholera, typhoid and other diseases in certain NATO countries before the outbreak of war.[1] The ultimate objective at the strategic level would be to undermine national resistance.

The operational level of UW supports front and subordinate army ground forces in depths that involve corps and echelons above corps rear areas. Since there is no requirement to linkup sabotage teams with ground forces as with airborne or heliborne forces, the depth of employment in support of the front could be as great as 1,000 kilometers (such a depth would be unnecessary in a European war). The missions of operational level forces would be directed and controlled by the front commander. The forces for this level could consist of different types, such as regular airborne forces with reconnaissance and sabotage missions, Main Intelligence Directorate (Glavnoe Razvedyvatelnoe Upravlenie or GRU) of the General Staff's "Special Purpose" (Spetsnaznacheniya or SPETSNAZ) units, and ground army sabotage/reconnaissance units.

The primary objective of these forces would be to destroy or neutralize nuclear weapons storage sites and delivery systems within the front's area of operations. Additional missions would include:

- Preparing and securing landing or drop zones for subsequent regular forces either heliborne or airborne.
- Providing intelligence on the disposition, strength, and activities of enemy forces.
- Conducting sabotage operations against airfields, railway lines, key bridges, communications sites, logistics facilities and other lucrative targets.
- Using assassination to intimidate the local populace and to eliminate NATO military leadership.
- Organizing local guerrilla or partisan groups for additional rear area threats.

Operating in the enemy rear area, unconventional warfare forces at the operational level will attempt to prevent the effective and timely employment of reserve forces, and will attempt to disrupt enemy offensive and defensive capabilities.

Tactical level activities are conducted in support of division and below with missions similar to the operational level. The depth of these operations would generally be less than 50 kilometers to disrupt friendly division and brigade rear areas. The forces used for tactical level would be airborne, army sabotage/reconnaissance units, and, to a very limited extent, the division reconnaissance battalion. The reconnaissance battalion of the motorized rifle and tank division has the primary mission of reconnaissance, but it may attack small targets of opportunity or conduct sabotage operations against nuclear weapons and logistics facilities.

Soviet airborne forces generally have wartime missions that are similar to those described above but are conducted in conjunction with and in direct support of units larger than division, attacking from the front lines with the tactical concept of link-up with ground forces in a relatively short time. The employment of regular airborne would be carried out by battalion up to division-size forces. This constitutes a rear area threat that requires a response by combat units. However, some airborne units have been designated and trained to carry out UW missions.[2] Conducting sabotage and reconnaissance missions behind enemy lines, these

company or smaller size units operating at the direction of the front commander would be separate and distinct from larger airborne operations and somewhat different from SPETSNAZ forces.

A force specially trained and smaller than the airborne units are the "special purpose" or SPETSNAZ units of regimental size or less, sometimes refered to as "diversionary brigades," subordinate to the GRU.[3] These elite units would not be employed as a brigade or regiment but in eight to ten man teams. Their main tasks include preparing for the landing of airborne units behind enemy lines, reconnaissance and real-time intelligence reporting on particularly critical targets, sabotage, disruption and even the use of nuclear, chemical and bacteriological weapons.[4]

In addition to the sabotage of specific targets and intelligence reporting, these forces offer tremendous potential for creating disruption in the rear areas by spreading news of disaster, changing directional signs, or inducing panic among refugees, causing them to move uncontrolled and to clog major road networks, road junctions and bridges. In short, they will do anything possible to create alarm and confusion in the rear areas.

These special purpose units of the Soviet army are more intensively trained than special airborne or ground forces. These saboteur soldiers will be dressed in the uniforms of NATO armies and will speak various European languages including English. Often their training is conducted in NATO uniforms with NATO equipment, serving to ingrain the habits and customs of their specific NATO force.[5] They possess extensive knowledge of the territory in which they are to work.[6] Among their specialized training is radio communications with burst transmitters, handling explosives, and unarmed combat.[7] They are also taught methods of surreptitious entry by picking locks, entering buildings silently through windows, and other techniques.[8] They learn survival techniques and can operate for extended periods on a minimum of supplies. As we will see later, this survival training serves to minimize a traditional vulnerability in the logistics requirements of saboteurs operating in hostile territory.

*A force specially trained and smaller than the airborne units are the "special purpose" or SPETSNAZ units of regimental size or less, sometimes referred to as "diversionary brigades," subordinate to the GRU.*

In addition to Soviet UW forces, we must count similar forces of other Warsaw Pact countries. These are estimated at approximately 20,000, primarily from East Germany, Poland and Czechoslovakia.[9] East German personnel, for example, will be extremely difficult to differentiate from West German soldiers. This situation provides a formidable threat that will not be easily neutralized.

Because these forces will be skilled in operating behind enemy lines, they will be well versed in clandestine methods of operation. The SPETSNAZ, in paricular, could work in conjunction with GRU "frozen" (zamorozhennye) agents, known in U.S. idiom as "sleeper" agents. Serving as guides, these agents could provide current operational information and logistics support to the sabotage teams. Local sabotage nets (KGB or GRU controlled) working closely with SPETSNAZ, could be particularly effective in neutralizing sensitive targets. For example, an operation to disrupt transportation networks could involve West German railways which are very vulnerable to attack at its electrical power source and automatic switching centers.

Both the KGB and GRU maintain links with and training facilities for Third World liberation groups and foreign terrorists. The links between these activities and the operations of Soviet SPETSNAZ are murky and difficult to define.[10] However, we must remember that Soviet partisan activities of World War II showed a willingness to apply terrorist techniques such as the assassination or kidnapping of high ranking German officers. Assassination or kidnapping of high ranking NATO officers would be just as useful.

The vast array of forces dedicated to operations behind enemy lines testifies to the gravity of the threat posed by Soviet and Warsaw Pact forces to rear area protection. The overall aim of UW forces will be to reduce efficiency of the defense by disrupting military rear areas. By creating such disruption, the Soviet advancing main forces are assured of a rapid, uninterrupted, and hence successful advance. UW operations in the enemy rear area will not in themselves be sufficient to bring about a Soviet victory; their task is merely to reduce the enemy's capacity to resist.

The threat posed by special purpose and other UW forces will not be easily countered. It can destroy objectives which are concealed or protected from most conventional forms of attack. This well-organized and specially trained threat will require comprehensive plans and dedicated forces for rear area protection operations. Within the fundamentals of rear area protection operations, as outlined in FM 100-5, the dimensions of UW are identified as Level I and Level II rear area threat activities. Level I includes activities of enemy agents, sabotage by enemy sympathizers, and activities of terrorist organizations. Level II includes diversion, sabotage and reconnaissance

conducted by tactical units smaller than battalions, primarily the UW forces outlined above. Although the rear area protection doctrine describes a Level III threat which is comprised of airborne, airmobile or amphibious forces—battalion size or larger—in the rear area. Intelligence and counterintelligence will have a diminished active role in neutralizing this threat which would require response by combat units. Army counterintelligence support will be primarily employed in countering Level I and II threats.

The sabotage and disruption role of the Soviet and Warsaw Pact UW forces is very similar to the effort tried by the German commandos under Col. Otto Skorzeny during the Battle of the Bulge in December 1944. Skorzeny had achieved a considerable reputation as a daring commando when he rescued Mussolini from the Italians. In his secret commando operation, named Grief (Condor), German soldiers of the 150th Panzerbrigade, in support of the Ardennes offensive, were dressed in American uniforms. Using captured American tanks, scout cars and trucks, small commando teams were led by officers fluent in British and American slang. These unique German soldiers were provisioned with suitcases of American dollars and British pound notes to bribe enemy guards or other personnel when necessary. During the German artillery preparation and initial assualt, they infiltrated the American lines and moved into the rear area to create confusion.

During the first two nights of the offensive, these saboteurs shot couriers, liaison officers and drivers; delivered false orders; erected barriers across roads warning of non-existent minefields; and attacked communications centers. Disguised as traffic controllers, they caused chaos for convoys. They set fire to fuel depots, built road blocks and even cut telegraph wires connecting the headquarters of Generals Omar Bradley and Courtney Hodges, commanders of American forces.

Fortunately, the German commando teams had received minimal training. They had been hastily organized, trained and dispatched only eight weeks before the offensive. Consequently, on December 18th, after only three days of operating in the American rear, a three-man team was challenged for a password and was unable to respond. They were arrested. This event alerted American forces to the magnitude of the sabotage threat in their rear area.

The threat was quickly rendered ineffective by increased vigilance and aggressive security in the rear area. Counterintelligence personnel and military police were on the roads day and night stopping personnel and suspicious vehicles. All suspects were held at gunpoint and with hands held high; they had to answer specific questions rapidly and without a trace of foreign accent. Passwords and documents were no longer a guarantee. These CI and MP patrols, along with sentries and other rear area security forces, would simply ask suspects, "In what state is Kansas City?" This would catch all but those German team leaders who had lived in the United States for some time. The ultimate success in neutralizing the effort overshadows the panic and confusion sown by such a small number of combatants. The actual effects were immeasurable and disproportionate to the German effort—the continuing historical mystique of these forces testifies to their residual shock.

A simple interrogation technique such as the Kansas City query will not assist the sentries of the next war against the sophisticated, well-trained SPETSNAZ soldier. The question would just as readily capture a real Dutch, German or other NATO soldier. Unlike their predecessors, the German commandos, the Soviet SPETSNAZ personnel have been trained well in advance of employment. Their organization and methods of operation have enough time to be refined, and their equipment will be state-of-the-art. The antidote for capturing or tracking down suspected saboteurs or sabotage teams will require comprehensive, dedicated counterintelligence support.

To counter this very sophisticated threat of unconventional forces, U.S. tactical units will require a complete integration of counterintelligence assets for support of division, corps and echelons above corps RAP operations. Rear area protection is designed to prevent enemy incursions into the rear areas, minimize the impact of incursions which do occur, and limit damage caused by such attacks.

Key to protecting the rear area from sabotage will be an intelligence preparation of the battlefield. A unit's CI analysis section will refine the G2's IPB for data to support rear area protection. Normal geographical analysis will identify infiltration routes, beachheads and groung avenues of approach. IPB will yield likely landing or drop zones and assembly areas for small teams. Generalized knowledge of the area of operation is not sufficient—an intimate knowledge of the operational area is essential. All important facilities and sensitive sites that would be lucrative sabotage targets for UW forces should be identified, located, catalogued and studied for "sealing off" actions in the event of reported attack. Likely avenues of approach to and from the identified targets, and from landing and drop zones, must be identified. The areas should be designated for aggressive patrolling and surveillance to provide early warning of rear area enemy activity. During the course of the battle, counterintelligence personnel working closely with the G2's all source intelligence center must be alert for ingress and egress air routes by noting suppressed friendly air defense systems that identify probable air insertions.

Insertion of UW forces can be made not only from the air but also on the ground. Infiltration could be easily accomplished through mass refugee movement, necessitating CI screening of civilian refugees and other line crossers from enemy territory for

*Key to protecting the rear area from sabotage will be an intelligence preparation of the battlefield.*

*CI personnel will be the most qualified asset for rear area protection commanders to expose possible SPETSNAZ cover stories.*

possible security threats. Cooperation with the military police is necessary to coordinate curfew laws and to control civilian refugee and evacuation movements. Other routes for ground infiltration that would accommodate small teams would be gaps between tactical units and rugged, seemingly inaccessible terrain. These areas should be routinely patrolled to guard against infiltration.

In addition to terrain analysis, a CI analysis of the threat can structure and determine the scope of the unconventional force order of battle. Along with information of UW forces, analysts can apply knowledge from past experiences in sabotage investigations. These studies have disclosed several weaknesses in organized sabotage groups that should be considered and used as guides in rear area protection planning and directing a search for saboteurs.

The first major step is to develop an analytic approach that will assist in identifying patterned operational behavior. The operational behavior patterns of sabotage groups will assume a definite modus operandi. This modus operandi is based on the characteristics of individuals or groups of individuals and usually is the result of previous sucess with a particular method of operation. This success will encourage reliance upon and a tendency to continue a favorable pattern. Initial successes will instill a false sense of security and stifle the formulation of new means.

Common errors committed by persons or groups engaged in sabotage or espionage activities which will establish a clearly outlined operational behavior pattern for the counterintelligence analyst or investigator include:

- Methods for contacting or rallying team members after an extended period will tend to be in the same manner and at the same place. This is done despite the teachings of most foreign intelligence services. Regardless of the possible risk of compromise and life, it seems to be a typical feature of human nature to establish a convenient routine or pattern for team members. This convenience creates a high risk of detection by counterintelligence forces.
- Repetitions of saboteur front line infiltration methods will compromise modus operandi. To a large degree, the methods for crossing battlelines are limited to gaps between units, during hours of limited visibility, within refugee movements, etc. Capture of a few saboteurs will establish some patterns and provide leads for analysis and investigation.
- For those UW teams in the rear areas with intelligence missions in addition to sabotage, the burden of reporting information will require a means of communication. Since timeliness of information is important, radios offer the best means of communicating. If not equipped with a burst transmitter, the long and continuous use of radios at certain times and locations will establish a pattern. Communication is a major weakness that will be discussed in more detail later.
- The execution of sabotage missions requires some preplanning to be successful. This will require reconnaissance or "casing" of a target location or facility. Sabotage teams could inadvertently set patterns in the methods employed to recon potential targets.

A second major area of weakness is communication. Communication difficulties include the necessity of maintaining communication between sabotage teams and their headquarters, sending reports in code which may be broken, the danger of location by radio direction finding units, and the transmission of reports which may be used as evidence by counterintelligence personnel.

Any information transmitted in writing is a potential clue which may fall into the hands of a counterintelligence agent. Codes and ciphers, photographs, maps and charts—the things most often set on paper, are the items most desired by the CI agent. These are the object of searching refugees, line crossers and other suspects.

Sabotage teams run the risk that their codes will be compromised by multiple use of the same code or confiscation by CI agents.

The possibility of direction finding forces the sabotage teams to constantly move. This need to find new transmission sites increases the risk of detection by CI informant nets or friendly patrols.

UW forces operating in the rear areas may attempt to recruit or work in conjunction with sleeper agents or local nationals creating a potential for another vulnerability—the risk of penetration by double agents.

Threat doctrine ascribes to the concept that except for initial equipment and supplies, special purpose forces are expected to live off the land. The logistics requirements may include acquisition of additional arms, explosives, food, and other items needed to carry out sabotage operations for long durations. The need for self-sufficiency increases the risk that UW teams will come to the attention of CI units working in rear areas; and hamper their ability to operate freely. In addition, more technical equipment required by UW teams would necessitate air-dropped or heliborne resupply. Alert CI personnel should track seemingly random or unaccountable flights into our rear areas for tips of UW team locations and for increased opportunity to apprehend or neutralize UW teams.

Beyond the contributions of analysis and exploiting weaknesses, CI personnel will need to accompany

military police and base defense force patrols on likely avenues of approach and in target areas to provide their expertise for initial screening and tactical interrogation necessary to uncover enemy UW forces in disguise. With European language training and a firm knowledge of the friendly situation, CI personnel will be the most qualified asset for rear area protection commanders to expose possible SPETSNAZ cover stories. For example, one based on an individual dressed in the uniform of one NATO force and claiming to be lost from another NATO unit. The seeking out of Level I and II threats is one of the most valuable missions for CI support to RAP operations: CI counters enemy intelligence, sabotage infrastructure, or other UW teams in the rear area.

CI personnel will also be able to enhance passive security measures of U.S. tactical units by conducting security evaluations and recommending countermeasures to base defense forces and sensitive sites. A key mission will be to actively check the use of passwords and countersigns in the rear area. This basic technique contributed to the initial capture and warning of the German commandos in 1944. Results from the National Training Center demonstrate that individual soldiers must be more conscientious about their security duties while acting as guards, tactical operations center protection forces, and while on other sentry duties. Opposing force personnel have been able to "kill" sentries or penetrate guard positions without being challenged or fired upon. CI assistance can provide an objective appraisal of rear services dispositions. Without adequate planning and safeguards, rear service units could locate various unit sites too close together or near likely infiltration routes. This crowded positioning allows for easy detection and large single strikes by sabotage teams.

Liaison with local governmental officials and indigenous persons known to be friendly to the U.S. will be useful in the establishment of informant networks. This will assist in monitoring unusual movement by strangers or seemingly friendly troops, for example, a Dutch soldier or three men in Belgian uniforms in a U.S. sector. Liaison with forest rangers, postal delivery workers, or local police would provide good sources for reports of strangers from the local populace. These liaisons will contribute to ferreting out highly skilled enemy forces.

Civil affairs actions which cut across all segments of society will provide many lucrative CI sources. CI personnel will have to work closely with the unit G5 for additional sources. In addition to the potential for sources, the G5's use of indigenous personnel for labor will require rigorous screening for agents and saboteurs. The Soviets used this modus operandi during World War II to infiltrate agents and saboteurs as drivers, cooks, or dining facility attendants at German headquarters. This gave their agents access to over-hear conversations, and the opportunity to steal or copy documents and maps, and to assassinate or kidnap senior German officers.

Although the general thrust of this article has been to look at the rear area protection problem from the perspective of countering the UW threat of Soviet and Warsaw Pact forces in a European scenario, the methods and scope of the CI role will be relied upon more heavily in a low intensity conflict with less sophisticated armies. In the low intensity environment, the problems for rear area protection become greater. We must remember the lessons learned in Vietnam and the requirements to secure a force in a conflict where there are no flanks or front—the rear area is everywhere. The demands on CI capabilities requires expertise in the application of counterintelligence techniques in various cultural settings, numerous language capabilities, and varying organizational structures at different echelons. Despite the magnitude of variations in the application of counterintelligence support from low to high intensity warfare, a firm doctrinal concept that identifies the scope of CI support to rear protection will provide a foundation that facilitates implementation.

The methods and expertise to neutralize Level I and II threats are provided by Army counterintelligence personnel. Therefore, when the commanders of rear area protection operations survey the battle area and organize their assets to accomplish the mission, they must know that counterintelligence is a prime contributor to countering the third dimension. ★

**Footnotes**

1. Aleksei Myagkov, "The Soviet Union's Special Forces," Soviet Analyst, January 9, 1980, p. 4-5.
2. Defense Intelligence Agency, **The Soviet Airborne Forces,** DDB-1110-2-82, April 1982, p. 4.
3. Chris Donnelly, "Operations in the Enemy Rear," International Defense Review, January 1980, p. 37.
4. Myagkov, p. 4.
5. Frederich Veiner, **The Armies of the Warsaw Pact Nations,** Carl Ueberreuter, Vienna, Austria, 1981, p. 153.
6. Myagkov. p. 4.
7. Aleksei Myagkov, "Soviet Sabotage Training for World War III," Soviet Analyst, December 20, 1979, p. 4.
8. Ibid., p. 4.
9. Donnelly, p. 37.
10. John Dziak, "Soviet Intelligence and Security Services in the Eighties: The Paramilitary Dimension," Orbis, Winter 1981, p. 782.

***FEEDBACK*** (continued)

*Headquarters USAREUR for its failure to satisfy the QMR.*

*QUICKFIX did not die with USAREUR's rejection. As years passed, memories have grown dim and further development has developed QUICKFIX into a platform capable of fulfilling the separate, equally vital requirement which Lt. Col. McColy represented. It would be a terrible mistake, though, to forget QUICKFIX' original purpose and fail to realize there's still work to be done.*

**Maj. Varon B. Mullis**
Hq USACC ODCSOPS
Fort Huachuca, Az.

**The U.S. Army Research Institute for the Behavioral and Social Sciences is a field operating agency of the Deputy Chief of Staff for Personnel. ARI researchers have been studying the human processes of intelligence analysis for 20 years and have been concentrating on the thinking processes of all-source analysis for the past 5 years. Some of their work on developing training materials for the new Tactical All-Source Intelligence Officer Course at USAICS was summarized in the April-June 1983 issue of MI Magazine. The October-December issue contained a study of IPB and procedures to assist the human judgment of intelligence analysis. This article, the final installment of the series, looks at how computerized judgment aids are used in IPB.**

# Intelligence Preparation of the Battlefield

## Computerized Judgment Aids

by Ruth H. Phelps

## Part II

***"Everyone complains of his memory, no one of his judgment."La Rochefoucauld***

Military intelligence analysts who have used Intelligence Preparation of the Battlefield procedures to predict enemy courses of action or avenues of approach are well aware that sound military judgment is fundamental to a good analysis. Acquiring good judgment is difficult and requires many years of military experience. This article will describe two new aids for helping analysts improve their own judgment capability to predict enemy courses of action.

Judgment aids are designed to structure the process of organizing and evaluating information, and integrate information into a final judgment. Judgment aids usually do not have tactical information imbedded within their procedures, since they are designed to be used in conjunction with another data source, such as a scenario, classroom exercise, or operational data base.

### Why Judgment Aids Improve IPB

The prediction of enemy intentions and capabilities requires the analysis of often unreliable and inaccurate information and indicators. The analyst copes with many data types and with undefined interrelationships between the information and the indicators, actual enemy intentions, and his or her own thinking processes.

There are six ways that judgment aids can relieve the analyst of some of the burden. Judgment aids can:

1. Provide a framework for organizing data so that it can be applied to any new problem.

2. Provide logical procedures for weighing the importance of both individual pieces of information and categories of information (such as terrain, and enemy reserves). Using a judgment aid requires **explicit** evaluation of information so that relevant information is not overlooked.

3. Provide logical procedures for integrating analyzed information into a single judgment, prediction or assessment. Often these are computerized procedures.

4. Provide the analysts with feedback about their evaluations (such as statements of the relative importance they placed on different factors or pieces of information).

5. Provide a vehicle for conducting personal wargaming in order to ask "what if" questions. Computerized aids can store many analyses simultaneously, so that analysts can, for example, predict enemy courses of action during both clear and rainy weather. In addition, analyses can be conducted and stored, based on assumptions. For example, "if blue forces attack, how will that change my prediction of the enemy?" or "what if they have three motorized rifle regiments instead of two?"

6. Provide a record of each analyst's or section's evaluations. These can be used to: evaluate a trainee's analytical strengths and weaknesses; compare two different analyst's evaluations; and communicate that background and rationale of an analysis to the commander.

Research conducted over the last 25 years in both laboratory and military environments has amply demonstrated that predictions of intelligence analysts are usually difficult and often impossible to make accurately. The most consistent finding of research on human predictions is that errors are not caused by lack of knowledge so much as they are by difficulty in using the information they **do** know in a reliable and consistent manner. Thus, judgment aids which help analysts to systematically evaluate and integrate information should improve the quality of judgment in the IPB process.

**A Decision Support Template Aid: ENCOA**

The decision support template is the standard intelligence estimate in graphic format. The analyst integrates assessments from early steps in the IPB analysis along with templates derived during the final threat integration step into an overall prediction of likely Enemy Courses Of Action. The ENCOA aid is designed to supplement this final step of the IPB procedures—making a prediction of enemy behavior.

The ENCOA aid is available to trainers and operational units in two manual versions: one is totally paper-pencil, and the other uses the HP41C or HP41 C-V hand held calculator. It is also available in two computerized versions: the IBM 5110/5120 computer in APL and the Apple II Plus computer in PASCAL.[1]

ENCOA aids assist judgment by breaking down the decision problem (predicting enemy mission accomplishment) into broad tactical factor categories and individual component factors so that each breakdown is more specific than the one preceding. Factor categories include terrain, U.S. forces, enemy forces, weather, and risk. These five categories are further divided into 25 individual factors, shown in Table 1.

Analysts perform five steps when they use ENCOA:

Step 1. Define COA. Analysts define which ENCOA will be evaluated in the analysis. Usually 2 to 5 COA can be determined.

Step 2. Evaluate COA. The analysts must evaluate the feasibility to the enemy commander of each COA on each of the 25 factors. ENCOA uses a relative scoring system: the best COA (from the enemy's point of view) on a factor is given a score of 100, the worst COA on that factor is given a 0, and other COA are given intermediate values. Figure 1 shows part of a sample analysis; note that the feasibility scores (values) for all factors would be listed by each category.

Step 3. Evaluate importance of factors. Specifying the relative importance or **weight** of the 25 factors is done in two phases.

First, the analyst assigns weights to the factors within each category separately. For example, the six factors within the terrain category are assigned weights corresponding to their importance relative to each other. The most important of the six terrain factors is given a weight of 100; the other five factors are given weights proportional to the most important factor (a factor 90% as important is given a weight of 90 while a factor half as important is given a weight of 50). Factors within the remaining categories are similarly weighted. Then the weights are normalized so that they add up to 100 within each category, as shown in figure 1 under the "Relative Terrain Weights" heading.

Second, the weight of each category is determined. This is done by comparing the relative importance of the categories for the enemy's mission accomplishment. A weight of 100 is given to the most important category; all other categories are weighted relative to it. Again, the weights are normalized to add up to 100.

Step 4. Calculating likelihood of COA. The feasibility scores of step 2 and the relative weights of step 3 are combined to obtain an overall value for each enemy alternative. These values are obtained by multiplying

**FACTORS IN ENCOA**

**I. Terrain Factors**

1.1 Field of fire afforded by terrain features.
1.2 Cover and concealment afforded by terrain features.
1.3 Mobility provisions due to terrain features.
1.4 Rapid seizure or denial of key terrain.
1.5 Observation provisions of terrain.
1.6 Accommodates natural and artificial obstacles.

**II. U.S. Force Factors**

2.1 U.S. disposition.
2.2 U.S. strength and condition.
2.3 U.S. reserves.
2.4 U.S. logistic support.
2.5 Probable U.S. actions/reactions.
2.6 U.S. command and control capabilities/vulnerabilities.

**III. Opposing Force Factors**

3.1 OPFOR current disposition.
3.2 OPFOR strength and condition.
3.3 OPFOR reserves.
3.4 OPFOR logistic support.
3.5 OPFOR command and control capabilities/vulnerabilities.

**IV. Weather Factors**

4.1 Observation/visibility conditions forecast to exist due to weather.
4.2 Cover and concealment conditions forecast to exist due to weather.
4.3 Mobility conditions forecast to exist due to weather.
4.4 Effect of extreme conditions of forecast weather on personnel and equipment effectiveness.

**V. Risk Factors**

5.1 Ability to cope with surprises in terms of U.S. strength or U.S. actions/reactions.
5.2 Freedom from dependence on forces not under own control.
5.3 Freedom from critical dependence on surprise or deception.
5.4 Suitability under unexpected adverse weather conditions.

**Table 1**

**Sample ENOCA Analysis**

| FACTOR CATEGORY: TERRAIN | VALUES COA¹ | COA² | COA³ | RELATIVE TERRAIN WEIGHTS |
|---|---|---|---|---|
| 1.1 FIELDS OF FIRE | 0 | 100 | 70 | 20% |
| 1.2 COVER AND CONCEAL | 0 | 30 | 100 | 16% |
| 1.3 MOBILITY | 100 | 10 | 0 | 5% |
| 1.4 S/D KEY TERRAIN | 10 | 0 | 100 | 25% |
| 1.5 OBSERVATION | 20 | 0 | 100 | 22% |
| 1.6 OBSTACLES | 0 | 100 | 90 | 12% |
| WEIGHTED SCORES | 12 | 37 | 88 | TOTAL = 100% |

**SUMMARY**

| FACTOR CATEGORY | VALUES COA¹ | COA² | COA³ | RELATIVE CATEGORY WEIGHTS |
|---|---|---|---|---|
| 1.0 TERRAIN | 12 | 37 | 88 | 40% |
| 2.0 ENEMY FORCES | 58 | 42 | 53 | 20% |
| 3.0 U.S.FORCES | 1 | 56 | 98 | 10% |
| 4.0 WEATHER | 34 | 42 | 68 | 5% |
| 5.0 RISK | 30 | 63 | 68 | 25% |
| TOTAL WEIGHTED SCORES | 26 | 47 | 78 | TOTAL = 100% |

**Figure 1**

the feasibility scores by their corresponding weight for each COA for each factor. If the scores and weights are valid and if ENCOA captures the factors most relevent to the situation, the enemy COA with the highest score is the most likely. For the analysis shown in the summary of Figure 1, COA³ has the highest score (78 vs 47 and 26) and is thus most likely.

Step 5. Sensitivity Analysis. When uncertainty enters the picture (and it usually does), it is of great importance to know whether variations in judgment would shift the final COA from one alternative to another—this is sensitivity testing. It systematically tests the sensitivity of the final COA scores to variation in the importance (weights) assigned to factors. For example, an analyst may have entered a weight of say 70 for a factor but was really uncertain as to whether that value might just as well have been 60 or 80. Sensitivity analysis is available only in the computerized versions.

Sensitivity analysis can also be useful when a group of intelligence analysts have conflicting opinions about the importance of particular factors. Sensitivity analysis reveals whether the differences in opinion significantly affect the final prediction. By calculating the importance of differences in opinion, ENCOA reduces emotional aspects of disagreement and encourages analysts to focus only on differences which truly make a difference.

Using ENCOA in IPB. ENCOA results in a numeric assessment of the relative likelihood of alternative ENCOA. The IPB decision support template requires displaying this assessment in graphic form. While the current form of the ENCOA aid provides this assessment numerically, the translation to graphics is quite simple. For manual overlays the numerical values can easily be recorded on the hand drawn graphics depicting the course of the enemy route on the map.

Most of the factors in ENCOA can be evaluated well before the battle starts; within the spirit of IPB, it can be used to prepare for battle. Once the battle begins however, new information must be incorporated. The aid described in the next section is designed specifically for the dynamic battlefield.

**Template Revision Aid: BAUDI**

Once the battle begins and new data are received, the templating process becomes dynamic and continuous. A decision support template, in fact, becomes obsolete as soon as new information is incorporated; the decision support template for one time period becomes the new situation template for the next. The BAUDI (Bayesian Aid for the Updating of Dynamic Intelligence) judgment aid is based on simple Bayesian decision theory and it has been developed to help intelligence analysts revise decision support templates. BAUDI is available in two completely computerized versions: Apple II Plus computer in the PASCAL language and; IBM 5120 computer in the APL language.[2]

Bayesian decision theory is a simple mathematical concept for logically integrating old COA likelihoods with new information to form a revised estimate. The Bayesian revision procedures are compared to the IPB templates in Figure 2. As shown, the IPB situation templates represent a current estimate of the enemy. The event matrix analysis assesses the impact of new information by matching the anticipated enemy events with actual events. Finally, in the decision support template, these two analyses are combined to yield a revised estimate of the enemy situation. As time proceeds and more new information is received, the cycle begins again and the decision support template becomes the new situation template to be integrated with the new battle-

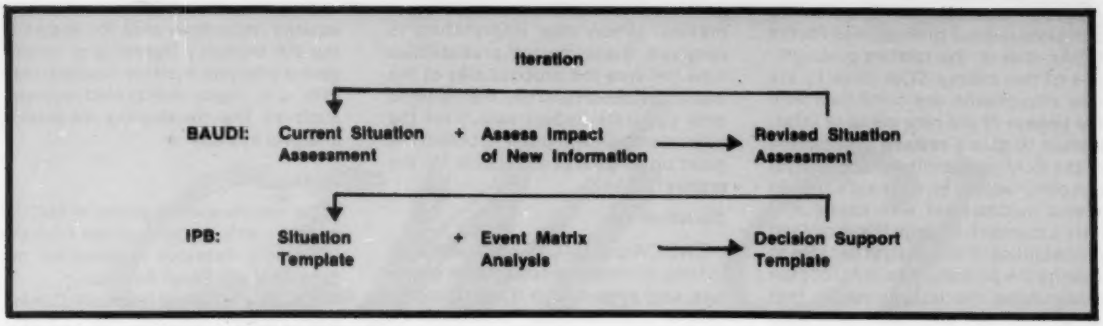



**Figure 2. Comparison of BAUDI and IPB steps.**

field information.

BAUDI assists template revision by adding structure to the process. The major task of the computer is to perform mathematical calculations which logically integrate the analyst's assessments in the situation template and the event matrix.

A critical feature of BAUDI is that it allows the analyst to disagree with the computer; the analyst can make numerical adjustments that seem more consistent with military judgment. BAUDI, however, then makes recalculations which show the analyst the logical implications of any adjustments. The analyst, however, always has the last input, not the computer.

Figure 3 shows the three major stages of BAUDI-aided analysis. The computer itself steps the intelligence analyst through the stages, clearly instructing the analyst on required inputs and its calculations. It is recommended, however, that the intelligence analysts using BAUDI for the first time should be familiar with the concepts outlined in Figure 2. The following description of BAUDI procedures assumes the goal of the IPB analysis is to predict enemy COA; however, the aid can be used just as well to predict enemy avenues of approach, mobility corridors, etc.

Stage 1. The analyst defines the number and names of the COA.

Stage 2. The analyst enters the relative likelihoods of the COA on the basis of all prior information. This is done by ranking COAs from most to least likely, and then specifying relative probabilities; that is, the analyst assesses how probable the most likely COA is compared to each of the other COAs. Ideally, the analyst would already have determined the relative likelihood of the COA by using ENCOA before the battle began.

Stage 3. The analyst uses BAUDI to assess both the impact of a new piece of information and the resulting revised situation assessment. For a given piece of information the analyst first enters a brief, identifying title. The analyst then specifies how many times as likely one is to see that information for the most likely COA as compared to each of the other COA.

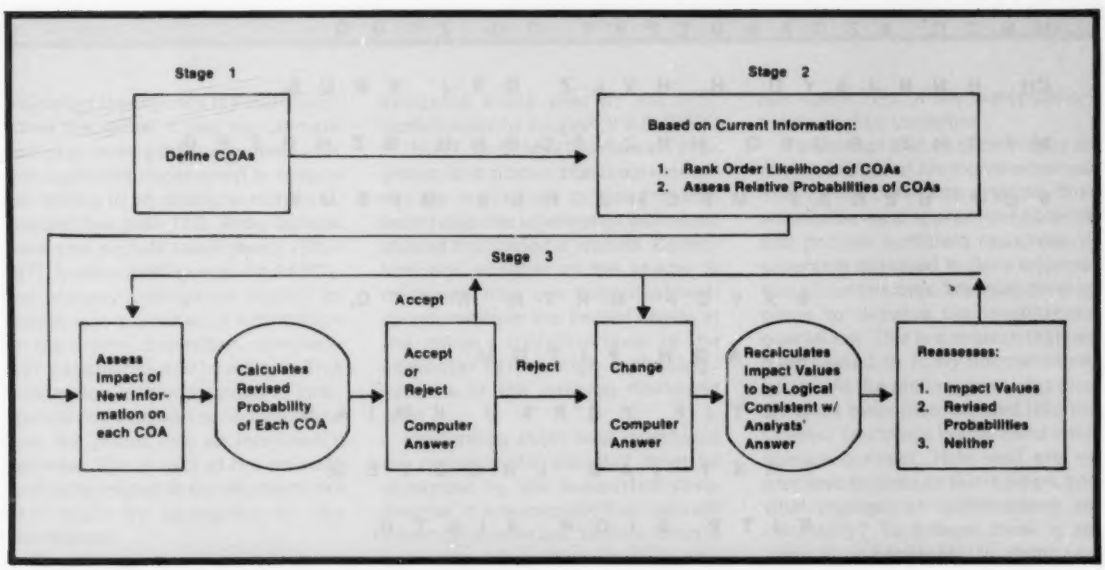



**Figure 3. The Baudi steps. All steps in boxes are done by the analyst; steps in ovals are done by the computer.**

BAUDI uses Bayes' Theorem to calculate revised probabilities for the COAs; that is, the relative probabilities of the enemy COA prior to the new information are combined with the **impact** of the new piece of information to give a **revised** assessment of the COA probabilities. The analyst can either accept or, if the aid's answer seems inconsistent with sound military judgment, change these revised probabilities. If the analyst decides to change the probabilities, BAUDI then recalculates the impact values that would have mathematically generated those probabilities. BAUDI also displays the original impact values so that the analyst can compare them to those calculated from the analyst's newly specified probabilities. The analyst now has the opportunity to change the impact values, if these appear to reflect too much or too little importance of the information being evaluated; if changes are made, BAUDI will recalculate the final revised probabilities. The iteration continues until the analyst is pleased with the impact values and revised probabilities for each piece of information. When new information is received, these revised probabilities now become the probabilities of the current situation and the analyst need only generate impact values for the new information in order to obtain the most up to date probabilities for the enemy COAs.

**Conclusions**

ENCOA and BAUDI were designed to help the intelligence analyst structure and systematize the judgments needed to prepare the IPB intelligence estimate. ENCOA is best used before the battle when there is ample time to carefully assess all the relevant order of battle, terrain and enemy factors. BAUDI supports the quick assessment required in **updating** an existing estimate in the midst of battle.

BAUDI and ENCOA are only two examples of very simple aids that can support the many areas of human judgment inherent in IPB. Additional aids need to be developed for use on microprocessors to support both classroom training as well as field and garrison operations. Perhaps equally important, aids for supporting the human judgments of intelligence analysis must be incorporated into any major automated system, such as the developing all-source analysis system. ★

**Footnotes**

1. For complete descriptions of ENCOA see the user's guides available from the U.S. Army Research Institute for the Behavioral and Social Sciences.
Phelps, R.; Hall, J. and Hoblitzell, C. **Intelligence Aid for Evaluating Enemy Courses of Action (ENCOA): Guide for Manual and HP41-C/HP41-CV Calculator Procedures**
Patterson, J., Phelps, R. and Hall, J. **Intelligence Aid for Evaluating Enemy Courses of Action (ENCOA): Manual for Use on the Apple II Plus and IBM 5110/5120 Computers.**
2. For a description of BAUDI, see Adelman, L.; Donnell, M.; Phelps, R.; Patterson, J. **An Iterative Bayesian Decision Aid: Toward Improving the User-Aid and User-Organization Interfaces. IEEE Transactions on Systems, Man and Cybernetics,** Vol 12, 733-743, 1982.

## Cryptocorner

*by Walter B. Howe*

*We challenge you with two cryptopoems in this issue. The first is very easy and should give you a good start. The second is much harder, but the substitution alphabet uses the same letter sequences as in the first. The letter substitutes are different in the second, because the sequences are lined up differently, but the similarities can help you if think about it.*

H N C G X F Q A H B E F V T C G Z V G Q

CH H N B J S Y U ' H H V L Z Q B J S B U E.

M F C H Z B U S Q H N Z F C E N H S Z H H Z F G,

V U Y U Z K Z F M F C H Z H N Z M F B U E.

B X Y C P D R T H K X T Q,

U B A Q H F I T Q U,

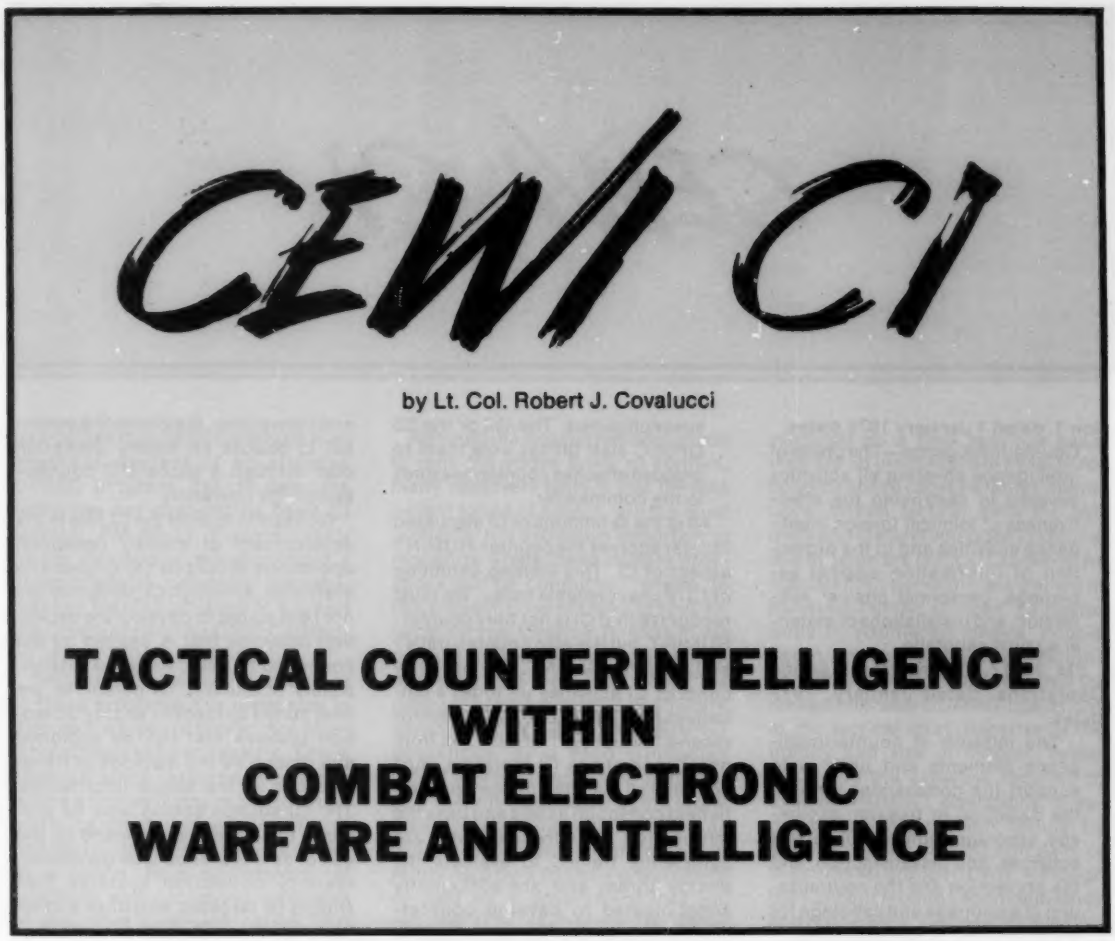
B X T I F Y Q R K U K M I A B.

F R K T I A B L R C O Y E U,

F I T P E I C W X I A T U,

A C B Y E H I A M T K R P B X Y U I A B.

(solution on page 43.)




by Lt. Col. Robert J. Covalucci

# TACTICAL COUNTERINTELLIGENCE WITHIN COMBAT ELECTRONIC WARFARE AND INTELLIGENCE

Combat Intelligence is a multifunctional discipline. It has the ultimate goal of providing the unit commander with sufficient information to reduce risk taking to an absolute minimum. Toward this goal, U.S. Army tactical units use signals intelligence (SIGINT), human intelligence (HUMINT), and imagery intelligence (IMINT) to collect vast quantities of information on the enemy disposition, composition, capabilities and intentions. This information is then provided to intelligence analysts who consolidate and fuse the pieces into an intelligence estimate. The quality of the estimate is directly related to the degree of risk that must be accepted by the commander.

Many thousands of words have been written by individual authors and by the U.S. Army Training and Doctrine Command. Billions of dollars are budgeted every year by the U.S. Government to support the SIGINT, HUMINT, and IMINT collection programs, and sizable analytical resources are maintained to fuse this collected data into intelligence estimates, studies and periodic reports. Collection and analysis of the enemy is designed into our organizational structures from the limited assets at the military battalion level to the computer driven high technology systems at the national command level.

Intelligence, at any level, must focus on reducing the risk that must be accepted by the supported commander. It is recognized that risks will never be eliminated. While a force is collecting information on an enemy, that enemy is simultaneously attempting to deny the collection of information and is involved in deception operations or the manipulation of information collected.

If we accept that we cannot deny an enemy the use of his multidisciplined intelligence collection systems, then we must develop appropriate doctrine and provide sufficient resources to programs designed to deny information to our enemies. We must develop plans to deceive his intelligence operations. This is a mission that has been tasked to Army counterintelligence. At the tactical level, this mission has been incorporated into the Combat Electronic Warfare and Intelligence concept. How well are we prepared to execute this mission, and what changes or modifications are necessary? To answer these questions it is necessary to determine what is expected and required of Army CI.

The Joint Chiefs of Staff Publica-


tion 1, dated 1 January 1979 states:

> Counterintelligence—The phase of intelligence covering all activities devoted to destroying the effectiveness of inimical foreign intelligence activities and to the protection of information against espionage, personnel against subversion, and installations or material against sabotage.

FM 30-17, Counterintelligence Operations, dated January, 1972 states:

> The mission of counterintelligence elements and units is to support the commander through the detection of treason, espionage, sabotage,sedition, subversive activities, and dissatisfaction, and the prevention and the neutralization of espionage and sabotage for the protection of the U.S. Army.

And, finally, let us look at a more timely treatment of tactical CI. FM 100-5, dated 20 August 1982, acknowledges that tactical CI includes countersabotage, counterespionage, internal security investigations as well as personnel and information security. Additionally, FM 100-5 states:

> Tactical CI supports OPSEC by identifying vulnerabilities and by eliminating or controlling the intelligence indicators susceptible to hostile exploitations. Intelligence support to OPSEC consists of developing and analyzing data on the enemy's intelligence—collecting capabilities and on friendly profiles. Such an analysis uncovers the sensitive aspects of a planned operation; determines essential elements of friendly information (EEFI) that, if known by the enemy, will compromise the operation; and assesses friendly susceptibilities. The G2 or the S3 OPSEC staff officer uses them to propose effective countermeasures to the commander.

All of the definitions of CI discussed thus far address the counter-HUMINT aspect of CI. This limiting definition of CI is unacceptable today. We must recognize that CI is not only counter-HUMINT, but it is also counter-IMINT and counter-SIGINT. To properly conduct CI activities on today's battlefield requires that the CI operator receive "all-source" information from non-CI operations. CI, therefore, must combine all the intelligence from battlefield collection assets and pass the information to individuals who are sufficiently trained to evaluate the enemy threat and are sufficiently sophisticated to develop countermeasures that can be taken by the supported commander.

In addition to the expanded multidisciplined CI definition developed above, it is necessary to clearly indentify and understand the CI role in tactical deception operations. Since CI is evaluating "all source" battlefield information and recognizing that most deception operations will be presented through multiple information sources, does it follow that CI should be responsible for indentifying deception operations? Or, is the identification of deception operations a responsibility for friendly deception operations? Most likely counter-deception analysis is an activity that must be directed by the G2 with constant interface between CI and order of battle personnel. If CI personnel are actively engaged in counterespionage, penetrations, or double agent operations they may be the conduit of deception information, and conversely, they have the potential to expose an enemy deception plan through a successful counterespionage operation.

An examination of the CI role in the development of friendly deception operations should be conducted and evaluated. Although CI personnel are not best suited to develop the deception objective that is desired by the command (a role clearly the responsibility of the G3), CI personnel are best suited to identify enemy collection systems that can be exploited and determine the methods of transmissions of the bogus information. The CI section should also be prepared to advise the command on the mix of data that should be generated, identify collection systems that should be targeted, establish a timetable for the release of the information, and conduct aggressive CI operations to evaluate the success of the operation during its execution. Added to the multidisciplined responsibilities of CI and its role in deception operations, we must also establish the CI role in operations security.

The treatment in FM 34-10, Military Intelligence Battalion (Combat Electronic Warfare Intelligence) (Division), dated 15 January 1982, treats the OPSEC mission performed by CI personnel assigned to the MI battalion much like FM 100-5. Additionally, both FM 100-5 and FM 34-10 agree that only through detailed OPSEC planning can effective deception operations be conducted. Thus, it is recognized that deception operations are dependent to a large extent on CI personnel who provide OPSEC support to the unit operations officer (G3/S3). As cited above, FM 100-5

# CEWI CI

recognizes that OPSEC analysis is an essential element of an effective OPSEC program. Yet, to date, the Army has not changed its basic CI manual, FM 30-17, Counterintelligence Operations, nor developed a comprehensive personnel management or training program to support the CI responsibilities OPSEC reflected in FMs 100-5 and 34-10.

Before looking at possible solutions to these problems it is necessary to discuss the types of conflict the Army is most likely to be engaged in. This is essential since resource constraints will be a driving factor in our doctrinal and force structure development. U.S. national policy clearly states that we, as a nation, have no intention of attacking and occupying territories of any other sovereign nation. Our forward deployed forces in Europe and Korea are deployed in a defensive posture and have the mission of maintaining peace and the current international boundaries. As recently as 26 April 1983, President Reagan stated on national television that the United States has no intention of committing its combat forces into Latin America. The Rapid Deployment Force concept, which has now mutated into Central Command, has a mission of confronting Soviet or Soviet surrogate aggression outside the borders of the Soviet Union and hopefully at the invitation of the violated nation state. U.S. Army forces are and most probably will continue to execute peace keeping missions at the request of the United Nations or as a result of U.S. initiated diplomatic actions. And finally, U.S. Army forces will be involved in countering terrorist activities both in the United States and overseas.

Although no attempt has been made to rank the above types of conflict, many observers believe that the less violent forms of conflict are the most probable. It is extremely important to recognize where these military operations will be conducted. Where, in this context, does not refer to specific geographical location. It refers to the political and motivational environment of the tactical area. Historically the most successful tactical CI operations, which by their nature, are HUMINT operations, have been conducted where there was access to partisans or a friendly population in the target area. The conflicts outlined above all will be fought in tactical areas currently held by a friendly government or held by a government that will request U.S. assistance. In either situation, it appears that enemy forces attacking an allied or friendly nation will be surrounded by a civilian population that will support U.S. objectives. This population will be in direct proximity to the tactical area of operation, and they clearly represent a lucrative source for "low level" HUMINT operations.

I submit that there is a pressing need to support tactical commanders with HUMINT coverage of the enemy second and follow-on echelon. But, the Army has no long-range reconnaissance patrol units and the target area is behind the deployment area of Special Forces units. The mission is not suitable for Ranger units, and the long-range surveillance outpost company proposed for the tactical exploitation battalion of the corps MI group (CEWI) has not been approved. Since we are concerned with tactical "low level" HUMINT operations that are of short duration and must be executed on a time sensitive basis they are an inappropriate mission for echelon above corps HUMINT operations. Within tactical units the soldiers who are best equipped to assume this mission are tactical CI agents. As indicated, CI personnel are trained in handling human sources. CI operations in counterespionage, double agent and penetration operations encompass all the skills required for limited offensive HUMINT operations at the tactical level. Because of the fluidity and size of modern battlefields and the expertise required to execute HUMINT operations, it appears that this mission should be assigned to the OPSEC company of the corps MI group (CEWI). Although the concept requires additional study and refinement, the need for this capability is apparent to even the casual observer of the AirLand Battle doctrine. Targeting requirements for second echelon and follow-on forces can not currently be satisfied by existing collection capabilities. However, this is essential since the targeting of the enemy second echelon is a critical component of the AirLand Battle concept. Without this ability we will be unable to judiciously allocate our limited weapon systems, interrupt the flow of enemy forces into the main battle area, or develop the battle lulls required to effectively conduct counterattack operations and to exploit enemy weaknesses.

In the tactical arena, "low level" HUMINT operations will use sources that have natural access into target areas. These sources may be refugees, line crossers, defectors or legal business people. Additionally, individuals may be spotted and assessed in peacetime without being ap-


proached or recruited until the time of conflict. Although I will not go into the details of the methods of operation, it should be understood that a source might be used for only one mission, receive very little training prior to employment, and may not be expected to return to his agent handler. This type of HUMINT operation should be controlled within the theater. Tactical HUMINT operations must be of limited duration and scope. Strategic and long-range HUMINT operations will continue to be conducted at echelons above corps. These operations will be subject to existing administrative and procedural restrictions.

Considering the "low level" HUMINT mission that I am recommending and the expanded OPSEC support role required of the CI agent, the tactical CI agent has an extremely important role to play in minimizing the risk that the commander must accept. To come to grips with this expanded HUMINT/OPSEC role for CI, fresh and innovative approaches to personnel management and training must be examined. Changes to our present systems may require modification of Armywide programs while others may be limited to the intelligence system. Linguistically proficient CI personnel are required for these types of HUMINT operations.

This is an area that demands a detailed evaluation of current Army programs. Consideration must be given to the development of a linguist procurement and retention strategy. This strategy must consider a career management program not only for CI personnel but also for the other Army intelligence occupational specialities that require language skills. For many years the Army has decried its inability to attract qualified linguists. Yet, there have been no major changes in our procurement or retention policy. The Army continues to throw money at the problem with dismal results. This problem directly affects CI operations. CI personnel should have second and in some cases third language proficiency to conduct low level agent operations, debriefings, liaisons, investigations in a host country, and support to OPSEC. Despite this, only 203 of the currently authorized 921 CI agent spaces are validated with a language requirement. The Army must take forceful action to solve the overall language problem. An officer linguist program should require all U.S. Military Academy cadets and ROTC cadets on scholarship to qualify in a foreign language prior to commissioning, require personnel in selected advance degree programs to qualify in a foreign language, and require intelligence officers in career field 36 to be qualified in a foreign language. Additionally, a career management field for intelligence linguists should be established to manage enlisted personnel. These personnel should be recruited, trained, and receive proficiency pay based on their language skills. Throughout their careers they will be assigned against validated linguist positions. As an example, if a linguist has been trained with a primary skill of voice intercept operator and is subsequently assigned as a CI agent, he or she will attend a CI training module between assignments. This program will help the Army capitalize on the perishable high cost skill of language proficiency and will also reward the soldier monetarily and professionally. This system of personnel management will provide the Army with a pool of linguists to meet quick reaction contingency requirements as well as MTOE and TDA requirements.

Another problem associated with the retention of linguist personnel has been the Army's inability to provide the soldier linguist with meaningful training, particularly in CONUS assignments. Yet, it is impossible to keep soldiers overseas constantly. Additionally, tactical intelligence units have a mix of both SIGINT and HUMINT linguists. In some areas there is an abundance of operational or training activities for SIGINT soldiers but none for HUMINT soldiers. In other situations (such as refugee support operations) HUMINT soldiers may have extensive requirements while there are none for the SIGINT operators. This problem can become tolerable if soldiers are recruited and paid with the understanding that the Army is hiring linguists. Currently, the Army hires SIGINT or HUMINT operators with possible or mandatory language school considered incidental. But, based on the Army's contract with the soldier, the intelligence skill is the primary recruitment incentive and special pay and reenlistment bonuses are predicated on the intelligence skill. No wonder a soldier is not anxious to become involved in second skill training, especially if it might mean a loss of pay. To counter this problem the soldier should be recruited and trained as an intelligence linguist. The initial language training should be based on Army language needs. Subsequent proficiency in additional languages should accrue special monetary bonuses to the


soldier. The significant difference in this system is that the soldier recognizes well in advance that language proficiency is the vehicle for promotion and monetary reward, and that the Army will determine in which intelligence skill or skills he or she will be trained.

The intelligence linguist CMF provides the Army with assignment and operational flexibilities that are impossible to achieve under existing linguist management systems. It also places up front the more difficult and most costly aspect of current SIGINT-/HUMINT training programs. Any soldier who fails to qualify at a certain level at the end of language training can either be released from duty or be assigned to a nonlinguist skill. For the CI agent, multiskill training will be extremely benificial since any assignment outside of CI will provide detailed knowledge of one of the multidisciplined aspects of intelligence required to conduct CI missions. Creating a force of 3,942 dual skilled military intelligence linguists is a quantum improvement over our present attempt to acquire 2,347 SIGINT linguists and 1,595 HUMINT soldiers who are not all linquists.

Critics of the intelligence linguist CMF will quickly claim that expertise in a specific phase of intelligence operations will be lost. To counter this problem the linguist CMF should have a mechanism to single track personnel at certain career bench marks. This program should also consider the development of a broad warrant officer program to ensure upward career mobility for linguist personnel. It must be recognized that the majority of the Army's force structure is concentrated at the tactical level. At this level the type of operations envisioned are less complex but more time sensitive.

The critical assumption in the adoption of an intelligence linguist CMF is that the language skill is more important for entrance qualification and career management than the skill for which soldiers are presently recruited and trained. Secondly, it must be proven that soldiers recruited as linguists are capable of being trained into intelligence specialties and cross trained into a second "utilization" skill. The Army must evaluate the present duty/work of linguists, retention profiles, and job satisfaction of linguists. Then, a study of an intelligence linguist CMF should be compared to our current system. A point that must be made clear is that a linguist CMF should not result in the formation of linguist units. A smooth transition from peace to war requires that soldiers be used in the duty positions in which they will find themselves in war. In addition to the development of unit team work and tactical skills, assignment of linguist personnel to tactical units ensures that they do not lose sight of their duties as soldiers. When assigned to a tactical MI (CEWI) unit the only distinction between a military linguist from an infantryman is a weekly program of linguist training and perhaps one 60-day peacetime utilization training period as part of the Readiness Training Program (REDTRAIN).[1] If we can fix the language acquisition system and expand CI operations to include offensive "low level" tactical HUMINT operations, have we fulfilled the expressed and implied missions that CI must perform? Can the CI agent accomplish the mission without specific help? Help beyond that which is presently available? We recently answered that question with a new program that missed the mark.

As a result of severe personnel shortages in the enlisted CI career field, a fix, known as the Counterintelligence Assistant Program, was initiated in January 1981. The goal of this program was to recruit 97B10 personnel as assistants to CI agents (97B20-97B40). The 97B10s that were recruited were sent to a 10-week training course at the Intelligence Center and School. Personnel were then assigned to tactical units. They were intended to help CI agents in investigative and OPSEC support functions, but they were not badge carrying, credentialed agents.[2]

Some have claimed that this program was the reincarnation of the 97D, CI Coordinator Program. The 97D was a CI clerk/typist and an all-around clerical support person to the CI agent work force. This program did produce many CI agents. But, in contrast to the 97B10 program, the 97D MOS was supported by TOE and TDA authorized spaces. The 97B10 program was not properly documented with appropriate doctrine and force structure support mechanisms. In the 97B10 program the soldier must serve only a one year minimum in a tactical CI/OPSEC assignment before he or she might be eligible for follow-on training as a 97B20, CI agent. Inadaquate and incomplete planning and staffing forced the suspension of the program in August 1981. What is noteworthy is the phenomenal appeal of the program in the recruitment phase. A similar program with equally, if not greater career potential, should result in similar success.[3]

# CEWI CI

It is often observed that U.S. government intelligence services collect more information than can be processed by our analysts. To compound this problem, Army intelligence has not developed an analyst to execute the OPSEC support mission assigned to tactical MI units. To effectively perform OPSEC analysis an individual must have knowledge of both friendly and enemy forces, must understand cause and effect relationships of information transfer on the battlefield weaknesses, and must earn credibility in the eyes of the commander and the unit staff. This is where we should place our money. The Army should develop, within the CI career field, positions and a training program specifically for OPSEC analysts. This training program must include the analytical techniques taught in current order of battle analyst programs, operating procedures and technical signatures of U.S. forces, deception and counter-deception techniques, and methods and procedures to reduce or selectively alter U.S. force signatures.

The mission of the OPSEC analyst must include:

- Understanding the enemy's intelligence collection systems and developing methods and sources to evaluate the success of his efforts.
- Learning the technical capabilities of the enemy's collection equipment and developing methods to reduce its collection potential or to deceive/alter information that is acquired about the friendly force.
- Understanding the doctrinal employment of the enemy's intelligence collection efforts.
- Maintaining files on the enemy's collection activities to include collection profiles of each collection means and pattern analysis, where appropriate.
- Knowing the method of operation, signature profile, operational tactics, and employment doctrine of friendly forces, to include allied forces that may be deployed on a flank of the U.S. force.
- Being fully knowledgeable on the area of operations.
- Conducting continual assessment and reassessment of friendly force OPSEC weaknesses and strengths.
- Providing insight and evaluation to deception operations.
- Functioning as the pseudo collection manager of the countersurveillance assets or programs of the command.
- Preparing other intelligence requirements for the unit collection plan that supports the development of the OPSEC data base.
- Recommending countermeasures to reduce or capitalize on friendly force OPSEC vulnerablilities.

The OPSEC analyst should be an entrance level recruitment skill. Upon completion of their initial tour of duty OPSEC analysts should be viewed as a source for CI agent recruitment. These personnel will be extremely valuable to the Army since they will have the analytical skill to complement their agent activities and to make them more effective in directing OPSEC analytical efforts and providing credible advice to the commander.

Upgrading the tactical CI/OPSEC capabilities of our forces is necessary to successfully execute the AirLand Battle Concept against a technically sophisticated and numerically superior enemy. These improvements will also enhance the security of U.S. forces in major contingency or low level conflicts.

Also, the OPSEC analyst skill must not be limited to tactical units. This expertise is as essential to echelons above corps as it is at the tactical level. Positions in TOE and TDA documents must be established prior to the implementation of this program. If force structure increases are not available to support this enhancement of intelligence units, then functional trade-offs must be made and spaces identified. A career progression profile of the OPSEC analyst might look like this:

The basic strength of the OPSEC analysts program is that it puts teeth into Army doctrine that is essential to force security. We must recognize that any doctrine requires appropriate support if it is to be effectively implemented. We have correctly identified the dangers of poor OPSEC, and history teaches us the value of deception and counter-deception operations. Additionally, we are recognizing the changing complexity of OPSEC in our technological environment. Knowing this, we are negligent if we do not resource the Army to counter the threat and to execute the OPSEC mission. The OPSEC analyst is not the total solution, but it is a major step in the right direction. With properly trained OPSEC analysts assigned to tactical MI units, required focus and expertise will be developed to enhance and better execute the mission.

There are many challenges in today's Army for all who are willing to work innovatively. As military professionals, we have directed our energies to solve problems with things that can be seen, weighted, quanti-

# CEWI CI

fied, and that give us a hard copy product. These bright and shiny gadgets are expensive, require constant upgrading to meet countermeasures technology, are bought in limited quantities (to the exclusion of war reserve stocks or reserve component units), and present maintenance nightmares on an extremely lethal battlefield. It is time we shift our focus to the human side of the equation. True, humans have warts and blemishes and often the product gained by human intelligence is not as easy to quantify, but its tactical impact can be spectacular. CI in the CEWI concept must not only achieve a multidisciplined defensive posture for the command, but it must also project an offensive HUMINT collection capability that is presently absent in Army doctrine. We can no longer hide our heads in the sand and accept that only 22 percent of the Army's enlisted CI spaces require foreign language training. We must establish an intelligence linguist career management field that will provide the Army with a more flexible, more economic, and more mission capable linguist force. This will require a revolutionary change in our current personnel management system. It will only be accomplished by people of vision who are convinced that correcting this current weakness in our Army is every bit as important as fielding the M-1 tank. In a time of massive modernization, additional changes to Army organizations or personnel systems are extremely unpopular, and rightfully so. But our linguist recruitment and retention problems have gone on too long; the lack of an up-dated CI doctrine for the field is necessary; appropriate concepts and resources to achieve our OPSEC goals are waiting to be fielded; and a tactical HUMINT collection effort is necessary to enhance our ability to execute the AirLand Battle doctrine. Properly addressed, these challenges will assist in the accomplishment of the ultimate goal of intelligence, the reduction of the risk that must be accepted by the unit commander. ★

**Footnotes**

1. Don E. Gordon, Lt. Col., "Soldier or Linguist?". **Military Intelligence,** Vol. 5, No. 2, April-June 1979, p. 44.
2. "The 97B Dilemma," **Military Intelligence**, Vol. 8, No. 4, October-December 1982, p. 50.
3. **Ibid.**

# Can Army Intelligence Better Support the Tactical Commander?

By Col. B.L. Lane

The U.S. Army's capability to position human intelligence assets to cover the increasing number of crises-prone areas of the world remains one of our major concerns and most difficult tasks. These areas of concern encompass not only the Warsaw Pact countries, the People's Republic of China, and North Korea, but also the emerging nations of the Third World. The political and economic instability in many of these lesser developed countries invites communism and other destabilizing influences that can easily precipitate conflict within and among these countries as well as simultaneously generating confrontations in other areas of the world. In this regard, one only need look to El Salvador, Nicaragua, and Honduras. Aggressively expanding communist influence and exploitation in these areas poses a serious threat to other countries throughout Central America as well as to the United States. The potential for this problem to spread to Mexico does indeed exist. Because U.S. interests may require the use of armed forces in many worldwide locations, Army intelligence must be professionally innovative and strive to improve our capabilities to provide intelligence support to deployed tactical commanders. A greater degree of HUMINT coordination and interoperability with our other intelligence technical collection systems, emphasizing the development and use of new technical aids and sensors to enhance HUMINT collection effectiveness is a means to that end. Army intelligence must fully participate within the intelligence community to plan and develop required intelligence capabilities in order to continue to meet present and potential strategic requirements in peacetime as well as providing full and timely support to tactical commanders in time of war. Unfortunately, we have fallen woefully short in this demanding arena. Long-range human intelligence planning, collection and integration has not kept pace with the rapid sophistication of warfare.

Since the end of military involvement in Southeast Asia, a revolution of sorts has been occurring in Army intelligence. New sophisticated equipment and new organizations have been developed and are now being fielded to provide more and better combat information and intelligence to our tactical commanders.

Other intelligence disciplines such as signals intelligence and imagery intelligence have continued to make great technological advances. The weakest link in the Army intelligence triad continues to be HUMINT, and specifically the orchestration of tactical HUMINT, which includes such things as POW interrogation, line-crosser/turn-around operations, agent nets, stay-behind operations, unconventional warfare, long range reconnaissance patrols, and long-range surveillance outposts.

HUMINT development has fallen behind, particularly in the areas of wartime doctrine and architecture at echelons above corps as well as at corps and below.

In contrast, overt and clandestine HUMINT collection operations in support of echelons above corps during peacetime are improving. These strategic HUMINT operations support theater and national level requirements concerned with early warning /imminence of hostilities, potential enemy plans/intentions, capabilities to wage war, and research and development. Army intelligence is a primary contributor in satisfying these stategic collection requirements and complements very capably our other national level stategic intelligence collection agencies. However, for Army intelligence to be able to adequately support the tactical commander in time of hostilities it is imperative that we expand our thinking as it pertains to tactical HUMINT during wartime. We have presently stopped short of what our tactical requirements and capabilities are in this combat support responsibility. FM 34-20, MI Group, Combat Electronic Warfare and Intelligence, deals with HUMINT only from an interrogation, counterintelligence and operations security standpoint. Chapters 6 and 7 in FM 100-5 are also deficient in their coverage of HUMINT support at echelons above corps, corps, and divisions and below. We doctrinally allude to integrating and analyzing information from all sources (ASIC /ASAS systems), but the doctrine is never articulated adequately. FM 100-5, as well as the planning guide AirLand Battle 2100 recognizes the enemy HUMINT threat to friendly operations and the need to counter this threat through aggressive counterintelligence. Our doctrine, however, never addresses the fact that we have that same HUMINT collection capability in our intelligence operational repertoire to use against an enemy. In chapter 4 of draft FM 100-16, HUMINT and controlled collection is again referred to only in general terms,such as where it fits into the intelligence support system of the echelons above corps intelligence center.

It is, therefore, quite evident that our tactical HUMINT doctrine must be readdressed. In addition to interrogation and line-crosser debriefings, other collection means such as clandestine agent nets, turn-around operations, clandestine stay-behind operations for target acquisition, augumentation and support to unconventional warfare operations, and passive reconnaissance (LRRP or LRSO) to satisfy commander/G2 collection require-

ments must be incorporated into a doctrinal update. The commander must clearly see the battlefield in order to fight effectively; and tactical HUMINT has a vital role to play in the intelligence preparation of the battlefield. Tactical HUMINT is a key element of combat power which supports the commander in the successful execution of the AirLand Battle.

Although HUMINT collection cannot be considered independent of our other collection systems, it is a vital part of the overall intelligence system. Our entire intelligence system is constructed to support the tactical commander by locating and identifying enemy movers, shooters, and emitters, and by identifying enemy "critical nodes" (key command, control, and communications systems/-centers). Tactical HUMINT is a key player in the system, and accomplishes its mission by locating enemy shooters before they shoot, enemy movers before they move, and enemy emitters before they emit. HUMINT, strategic as well as tactical, has a unique capability to determine enemy intentions, capabilities, and combat effectiveness, a recognized difficult task for signals intelligence and imagery intelligence.

Our present doctrine simply reflects that we have placed too much emphasis and reliance on technical collection in general, and in the HUMINT arena, too much emphasis on techniques such as collection through official cover, in particular. Official cover collection such as embassies and attaches, will be practically nonexistent during wartime. And when our technical collection systems are neutralized, constrained by good enemy security practices or by a "dirty" battlefield, human agents then become the vital element in the intelligence collection system to fill the gap for the tactical commander. However, we cannot wait until hostilities start to recruit these valuable assets. This is a tedious process that must be planned and executed well in advance of hostilities. It requires foresight and meticulous contingency planning. Moreover, it demands a realization at our national level (the Director of Central Intelligence, the intelligence community staff, the services, and the Intelligence Oversight and Appropriations Committees in Congress) of the necessity to start preparing now to incorporate this type of HUMINT collection into our overall peacetime defense policymaking posture, both stategic and tactical. We must cause our bureaucracy to be provocative in their thinking and to approve Army intelligence planning and funding for long-range tactical HUMINT, to be able to make the transition from peace to war in support of the tactical commander. It must be fully recognized that HUMINT has a day-night all-weather capability. We must develop a HUMINT capability for support during wartime. Our tactical HUMINT doctrine has just not kept pace with the need and the requirements set forth in the Army's new fighting doctrine.

The AirLand Battle is an operational concept for warfare, applicable for mid to high intensity conflict. The concept deals with the orchestration of all available intelligence and combat assets, employed throughout the theater battle area, to disrupt enemy efforts to maneuver and mass his forces, and to engage and destroy the enemy under conditions favorable to friendly forces. Implementation of the concept requires the ability to "see deep" through exploitation of accurate and timely intelligence; "to strike deep" through precise application of firepower throughout the enemy's area of operations; and to mass all available combat power against the enemy at the decisive time and place. No realistic tactical HUMINT planning has been undertaken to support the AirLand Battle Concept. HUMINT collection units in the Army are not ready to go to war. Former Defense Secretary Harold Brown said, "If you're going to do maneuver warfare, you need better command and control. You need to locate yourself. You need information on where the other side is." HUMINT, in concert with our technical systems, can tell the tactical commander where the other side is.

Army intelligence, as well as the entire intelligence community, is aware of our wartime collection requirements but we're only giving lip service to HUMINT collection. Army intelligence, at present, is not fully prepared to meet the commander's continuing intelligence needs in wartime. We can improve our capability, however, by reworking our tactical HUMINT intelligence doctrine. Initiatives are underway in the Office of the Assistant Chief of Staff, Intelligence and the Office, Deputy Chief of Staff for Military Operations, Department of the Army, to correct these shortcomings. As these initiatives take shape, support will be required not only from the military intelligence community, but from the Army as a whole.

With these things accomplished, we can go to war and do the job. ★


FOR
MANU
ARMY
KRISANO
Military Intelligence

# AMERICA'S
# ORGOTTEN
# WARS

by Kevin Lamere

**The foregoing analysis is in response to growing "rumors" that the guerrilla trainer and fighter is no longer a strategic asset. The objective of this analysis is to illustrate that nothing could be further from the truth; witness El Salvador, Afghanistan, the Philippines, Kampuchea, and Thailand, just to name a few. Guerrilla warfare is the most cost-effective, most tactically sound and the most destructive form of warfare being waged today. Ironically, guerrilla warfare was also the first form of U.S. warfare. United States history reveals that the art of guerrilla warfare has been proven and refined right in this country.**

United States foreign policy toward popular insurrection or "people's wars of liberation" since Vietnam has been vague and inconsistent. The past administration wanted to aid Morocco and Pakistan against communist inspired insurgents. Counter-insurgency techniques are being revived in U.S. policy toward Central America. There is a movement in Congress and around the country to aid and train Afghan guerrillas to fight against the Soviets. This is an ironic turnabout of the past decade. Guerrilla warfare and terrorism seem to be everywhere, from the streets of Belfast to the dusty backroads of Namibia and Angola. How the United States can respond to this dilemma remains a mystery.

The United States needs to form a cohesive and comprehensive long term "strategic consensus" so that its basic directives will not change with every new public opinion poll or administration. It must address long term efforts or short term tactical "quick fixes," to offset Soviet long-term strategic goals, which remain firm. This policy has the United States stepping from one crisis situation to another. During the past two administrations, the United States has not been without a crisis on its hands.

The United States must develop a "strategic consensus" towards insurgency and retain its primary objectives, regardless of changing political winds. Today, there are at least 37 ongoing armed conflicts in the world, some of recent origin, others dating back decades. In these wars, over 8 million combatants go on fighting for causes with which most Americans have little familiarity. These are guerrilla wars fought by local or sectional nationalists for a variety of causes. In terms of actual military capability guerrilla armies are inferior to conventional armies yet cannot be quelled by them.

American opinion instinctively recalls Vietnam as the latest counter-insurgent war. However, the historic record predates Vietnam by centuries. It is unlikely that more than a handful of military professionals are aware of this part of our history. Most Americans are familiar with the popular wars of history, with the total

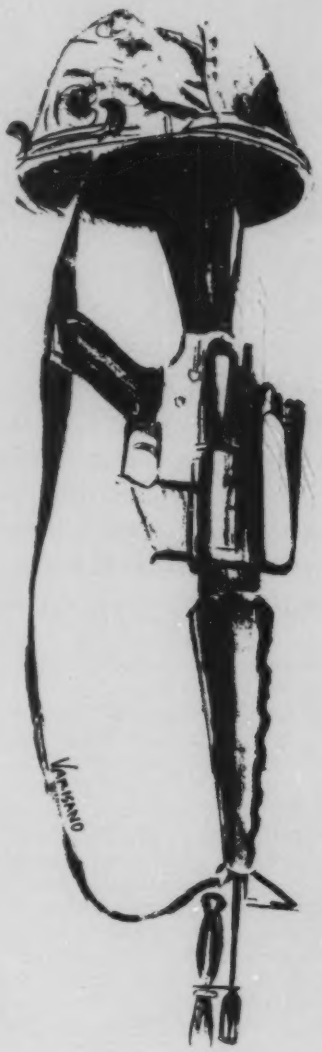
mobilization of men, resources and technology, and the traditional American faith in quick military victory.

Far less known, but perhaps more relevant at this point in time, are the other wars in the United States' past; those involving guerrilla warfare and terrorism, where the conventional use of armed forces didn't work. The military conducted frustrating and brutal operations against civilian populations, often contrary to public opinion at home. The Vietnam war was not a unique experience in U.S. history.

If the present administration is serious about a "tough" foreign policy towards Third World intervention by the communist bloc, an historic glance at "toughness" in guerrilla warfare situations should prove sobering. U.S. military history is rich with examples of irregular warfare with U.S. soldiers and citizens in roles as guerrillas and anti-guerrillas or counter-insurgents. Each role has contributed to the forgotten American heritage of guerrilla warfare and terrorism, an unpopular subject, yet one that must be addressed. It also promises to be around for the forseeable future.

When our country was young, Americans often fought as irregulars, especially in the South. This is where the greatest degree of guerrilla warfare and terrorism took place. Armed invasions of the South, first by the British in the Revolutionary War and then by the Union in the Civil War, furnished ideal occasions for the use of guerrilla warfare by the Americans. These early partisans waged long and vicious paramilitary campaigns especially during the Revolutionary War when bands of "Whigs and Tories" fought full scale terrorist wars against each other, almost completely independent of the military campaign. The war in the South was almost completely guerrilla in character, especially in Georgia and the Carolinas where much of the population supported Great Britain. Terrorism was a common feature of everyday life with lynching parties, murder, ambushes, and sabotage.

During the Civil War, Union armies were faced with the task of eliminating southern guerrillas led by John Mosby. They were no more accustomed to irregular warfare than most conventional armies, before or since. Gen. Grant's reaction to Confederate guerrilla raids in Virginia was typical of West Point thinking. Reflecting the frustration of the regular officer forced to fight guerrillas on their own ground, Grant issued (with Lincoln's permission) the following orders to Sheridan: "If you can spare a division of cavalry, send them through Loudon County to destroy and carry off the crops, animals, negroes, and all the men under fifty years of age capable of bearing arms. In this way you will get rid of many of Mosby's men. Give the enemy no rest. Do all the damage to railroads and crops you can. Carry off stock of all descriptions, and negroes, so as to prevent further planting. If the war is to last another year, we want the Shenandoah Valley to remain a barren waste."



Grant's brutality in eliminating Southern partisans was followed to the letter by Sheridan, methods which later became notorious when Sherman ravaged Georgia. Sheridan's tactics in the Shenandoah Valley have become stock-in-trade for regular soldiers when fighting guerrillas who have the support of the populace. When he was finished, Sheridan left the Shenandoah Valley residents, in his own words, with "nothing but their eyes to weep with." Tragically, this is the fate of people who must face the vengeance of conventional armies in pursuit of elusive guerrillas. This experience was to be repeated over and over, not only in Virginia, but in the Philippines and wherever else U.S. soldiers met hostile populations in support of irregular forces. Grant's strategy of "annihilation" (going to the heart of the enemy in the shortest possible time with the greatest amount of men and material) has since come to symbolize the ideal of U.S. warfare. His tactics against Southern guerrillas may have been barbaric and awkward, but they worked. The Civil War pushed the United States into the forefront of the world's military powers.

The first major U.S. Army expedition against guerrillas took place years before the Civil War. The Seminole War was one of embarassment and frustration and was a lesson forgotten as soon as it was over. The war was fought in the Florida Everglades, where the Army tried to remove the Seminole Indians from their homes onto reservations west of Arkansas. It has been described by experts as the largest, most costly and frustrating Indian conflict in U.S. history. Although the Seminoles had less than 1,000 braves, they managed to hold out for seven years (1835-1847). Before the war was over, 1,500 American soldiers had lost their lives, more than in all other Indian wars combined. The cost of the war reached $40 million, a staggering sum in those days. 10,000 troops plus some 30,000 volunteers saw duty in Florida under eight different commanders.

Americans quickly tired of the

campaign, after no quick results were evident. Criticism mounted against the Army's tactics; using bloodhounds to search for retreating Indians provoked dissent from Northern humanitarian groups. As the war deteriorated into slow-moving search operations, the lack of visible success in battle tired the American public. By now, Americans were accustomed to judging military affairs purely in terms of victory in classic battle maneuvers. The Seminole War offered none of this. The tedious process of searching vast swamp areas to find small Indian camps was unpopular with the American public and the volunteers. Mounting cases of tropical disease and death led to short enlistments and subsequent recruitment problems. In the end, the Army won the war by adjusting its strategy. It learned that it could not win with heavy columns and logistics lines. The key was the result of strategy devised by Colonel William J. Worth, who struck the Achilles heel of every guerrilla force: its support network.

Worth led his men against the settlements and crops of the Seminoles, destroying their means of subsistence and preventing them from raising and harvesting future crops. His troops suffered extensively from sickness, but it worked. Except for a few diehards, the Seminoles ended their opposition to U.S. authority and agreed to resettlement in 1842.

The Philippine insurrection of 1899 to 1902 is still the best case study of the American military in a counter-insurgent role. After Admiral Dewey's victory in Manila Bay, the Spanish army on land surrendered and the U.S. troops occupied Manila and the surrounding area. By then, a native independence movement had been formed around Emilio Aguinaldo, a 29-year-old revolutionary. Aguinaldo assembled an army of almost 80,000 and became disenchanted with U.S. treaty terms and laid plans to forcibly evict the American Army. The battle for Manila began on February 4, 1899, when Aguinaldo's army charged straight at American positions. The next day, Aguinaldo's army was in full retreat after suffering 2,000 to 5,000 casualties, compared to 59 Americans. This defeat impressed Aguinaldo with the impossibility of defeating the Americans with conventional tactics.

The American command believed the insurrection was over. Gen. Elwell S. Otis, the U.S. commander, refused to believe it was anything more than a tribal revolt; confidently, he reported that the rebels had been crushed. Throughout 1899, Otis maintained his military and political perception of the situation. Rather than occupying territory, he ordered his men back to base, during which time the insurgents were allowed to regroup and reoccupy the area they had vacated earlier. It was not until late in 1899 that American forces ventured beyond 60 miles of the capital. The fact that the rebels were forced to go underground gave the American command the impression that the war was over. In reality it had only begun. Aguinaldo's full conversion to guerrilla warfare was completed in November 1899. For three years thereafter, his men engaged a total of 125,000 U.S. troops in a protracted political-military campaign. It dragged on with no visible success until President Theodore Roosevelt formally declared it over on July 4, 1902. Like most guerrilla movements that fail, this one didn't simply end, it just simmered down to a tolerable level until it finally faded away. It left 220,000 dead Filipinos, 4,234 dead Americans and a bill of over $500 million.

Yet the Philippine insurrection, even by 1902, was not yet over. No sooner had most of the main areas been pacified, then it became necessary to calm down the provinces immediately south of Manila, where over 5,000 insurgents led by Miguel Malvar had re-established their authority.

In a campaign led by Gen. J. Franklin Bell, U.S. forces moved into southern Luzon to stay. Using early "strategic hamlet" concepts, Bell discarded any notion of a policy of "attrition." He instituted a policy of reconcentration of all natives presiding inside the designated areas. Neutrals were not tolerated. All Filipinos were designated as either friends or enemies. All enemies, of whatever age or sex, were to be killed or captured. All friendly citizens had to move into zones established by the military. Those found outside the zones would be shot on sight. The local police were disarmed and a 2000 to 0800 hour curfew was strictly enforced.

Whenever an American soldier was killed, a Filipino prisoner was randomly selected and shot. Whenever


Army property or telegraph lines were destroyed, a Filipino village was razed. Outside the designated areas, Bell went after the remaining guerrillas with a vengence. Troops scoured the countryside, systematically confiscating all food and military supplies uncovered. In one province alone, 54,000 civilians perished of either epidemics or starvation. Bell's men pursued the retreating guerrillas relentlessly, not giving them a second to relax. Without access to either supplies or native support, the resistance movement completely collapsed. The Americans conducted a devestatingly brutal counter-insurgent campaign; but one that was eminently successful.

The American's remedy for the insurgency provoked strong opposition on humanitarian grounds. Similar opposition has been present in every American counter-insurgent campaign ever fought—past, present and probably future.

For example, a statement by Senator George F. Hoar, intervention critic from the beginning, "What has been the practical statesmanship which came from your ideals and sentimentalities? You have wasted six hundred millions of treasure. You have sacrificed nearly ten thousand American lives, the flower of our youth. You have devestated provinces. You have slain uncounted thousands of the people you desire to benefit. You have established pre-concentration camps. Your generals are coming from their harvest, bringing sheaves with them, in the shape of other thousands of sick and wounded and insane. Your practical statesmanship has succeeded in converting a (grateful) people into sullen and irreconcilable enemies, possessed of a hatred which centuries cannot eradicate."

Except for the year and American dead, the statement could have been

used by anti-war activists in the 19th, 20th or 21st centuries. U.S. military missions against guerrilla opponents only began with the Philippines. Most others were much smaller with fewer casualties and less public outcry. Some went completely unnoticed by the U.S. public, because then press censorship was a standard feature of U.S. counter-insurgent doctrine. It was an era when U.S. leadership offered no apologies for the show of military power, the issue of morality went unquestioned. We were to repeat the same mistakes over and over again in every insurgency we fought.

General Pershing's campaign against Pancho Villa's villistas provided clear examples of a military leader being held back by political restraint. President Wilson restricted Pershing to within 150 miles of the U.S. border.

Pershing called Washington, "If this campaign should eventually prove successful, it will be without the real assistance of any natives on this side of the line."

This policy was to be repeated with the institution of the 17th and 38th parallel restrictions in Vietnam and Korea.

In 1919, Marines were sent to Haiti to quell the "Caco" revolt, composed of war-like ex-slaves, led by a charismatic leader known as Charlemagne. They organized a resistance movement against the U.S.-created Gendarmerie during the summer and fall of 1918. The Cacos developed a force of 3,000 with the active assistance of at least one-fifth of the population. This was accomplished by a system of murder, terror, blackmail, and intimidation against the civilian populace. The movement gradually assumed the proportions of a full-scale revolution aimed at the complete withdrawl of U.S. troops. The country teetered on the brink of disater. In March 1919, the government asked for full scale intervention to save the country.

Militarily, the Cacos were careful to stay away from the main body of the Marine strength, with two exceptions. Between April and September 1919, the two sides engaged on over 100 occasions, sometimes in pitched battles, but usually in small skirmishes. These skirmishes often resulted in the retreat of the insurgents into the countryside. However, a premature attack on the capital city of Port au Prince ended in disaster and set the movement back considerably, but did not end it.

The end finally came when Marine Sgt. H. Hanneken, disgusted with inaction by his superiors, disguised himself with black cork and, along with his corporal, went undetected through more than six Caco outposts. When a Caco turncoat, by prearrangement, pointed out Charlemagne near a small campfire, Hanneken shot the elusive guerrilla leader, killing him instantly. His bodyguard was killed by the Marine corporal, William R. Burton.

After the loss of Charlemagne, insurgency in Haiti declined rapidly. The Marines divided the country into areas of responsibility and systematically searched out remaining guerrillas. Within six months, over 3,000 Cacos had either turned themselves in under protection of the government's amnesty program, or had been killed in relentless pursuit by Marine patrols.

The Dominican Republic in 1916 paralleled Haiti in many aspects: a radical revolt using blackmail, coercion, murder and terror to extract support from the civilian population. The Marines tried fruitlessly for five years to crush the insurgency, and then in desperation decided to experiment with a system of "cordons" to rid the eastern part of the country of active partisans.

In effect, the American cordon was a total war against the insurgency. Large numbers of U.S. troops blocked off an area of the country and rounded up every adult male for a series of mass line-ups in which concealed informers would identify known insurgents. After five months, this yielded more than 600 convictions. The United States also undertook the training of a number of Dominican Guardia in anti-guerrilla tactics. Only Guardia members that had previously suffered at the the hands of the enemy were selected. They were organized into special anti-guerrilla outfits and sent on small patrols. The Dominican "Special Forces" had several contacts with the guerrillas, most of them highly successful. This, along with stepped up Marine patrols, effectively ended the guerrillas as an political and military force in the republic by May 1922. Complete pacification of the countryside was soon in coming.

Many examples of guerrilla warfare being successfully fought by the United States are recorded in history. We need to draw upon lessons from the past in order to prevent costly miscalculations in the future. Vietnam was an attempt at counterinsurgency in its early form. Events of the war soon compelled the military to return to conventional tactics and heavy fire power, especially after the fall of the Ngo Dinh Diem regime. History proves conventional military power can be extremely effective against a popular based guerrilla force, but only if matched by an iron political will, which will not hesitate to employ total control over the entire population, both military and civilian. Americans have also learned, through years of frustrating trial and error, that mastering counter-insurgent techniques requires an uncommon ability in police, administrative and political skills seldom taught at military academies. These techniques are learned "on the job." Also, in all guerrilla wars of the past, without exception, Washington has not been willing to appreciate the deep cultural roots of the invisible enemy, his motivation, or his political sophistication. The American view of warfare is one of uniformed enemies locked in open combat on battlefields, with the issue decided by the use of massive strength and conventional deployment and tactics. This view is irrelevant against guerrillas as U.S. troops have had to learn, time and time again. The U.S. public has little tolerance for military actions against indigenous guerrilla forces, especially when such actions go on indefinitely without visible success, as most do. These problems in Vietnam, for example, were magnified many times over by the constant searching eye of the television camera and the critical news media which, we had previously learned, needed to be censored in a protracted, brutal guerrilla campaign or we could not win. U.S. military leaders had to conduct a war in full view of the U.S. public. Future wars will undoubtedly magnify this mindset of U.S. technology to broadcast even the most sensitive details of military operations. Today, counter-insurgency is a lost art in U.S. strategy. Only a few years ago, there was talk of deactivating the 7th Special Forces Group.

This neglect to train and prepare of unconventional warfare situations may force the United States to repeat historical mistakes. The U.S. must recognize the fact that revolutionary, guerrilla and terrorist warfare is a permanent feature of the strategic environment of the future. The problem is not budgetary; effective counter-insurgency is the most cost effective strategy in the U.S. arsenal. The major problem is cutting across the overlapping U.S. military and civilian agencies in order to arrange a centralized and localized control system for future insurgency. Common tactical doctrines and a streamlined command and control system are essential if the pitfalls of the past are to be avoided. If this is not recognized and acted upon, the United States will have no choice but to turn away by default from the rising tide of radical and extremist political movements that promise to dominate the remainder of "free" governments and almost invariably choose to wage unconventional was against established allied governments and peoples. Indeed the trend has begun.

Maj. Gen. Edward G. Lansdale (USAF retired), a noted expert on revolutionary war, has warned, "We live in a revolutionary era. My hunch is that history is waiting to play a deadly joke on us. It did so on recent graduates of the Imperial Defence College in London who now find themselves facing the savagery of revolutionary warfare in Northern Ireland. It did so on Pakistani officers under General Nizai, who undoubtedly wished that they had learned better ways of coping with the Muki Bahini guerrillas. It is starting to do so on Argentine graduates of the Escuela Nacional de Guerra in Buenos Aires who are waking up to the fact that Marxist ERP guerrillas intend to win themselves a country with the methods of the Tuparmaros next door."

It is time the United States recognizes the significance of unconventional warfare, and the need for appropriate and modern countermeasures. If American administrations intend to involve this country in future insurrections, either in support of an allied government or to aid anticommunist guerrillas, its first set of lessons should derive from a forgotten American heritage. ★

# SUMMER INTELLIGENCE SCHOOL


The 37th annual Fifth Army Area Intelligence School is set for two-week sessions June 10 to Aug. 3 at Fort McCoy, Wis., its 18th year at this training center.

Conducted by the Headquarters Fifth Army intelligence and security office and staffed by Army Reservists, the school provides intelligence training each summer to Reserve Component personnel, with emphasis on intelligence military occupational specialty qualification. There are also specialized, non-MOS producing course. All are accredited by the Army Intelligence Center and School at Fort Huachuca, Ariz., and closely parallel those courses.

Following are this year's courses: Tactical Intelligence Officer (SC 35A); Intelligence Analyst (MOS 96B, 964A); Counterintelligence Officer/Technician/Agent (SC/MOS 36A, 971A, 97B)—three two-week phases; and Phase IV, the 9IGSEC phase exclusively for Counterintelligence Officers (36A). Also, three unphased courses—S2 Combat Operations, Communications Security (COMSEC) Custodian, and Security Management.

The nearest commercial air terminal is at Lacrosse, Wis. For more information, call Joe H. Lopez or Maj. Frank O. Riggs, AUTOVON 471-4907/2610 or (512) 221-4907/2610.

# FIELD TRAINING PROGRAM FOR CI ASSISTANTS

by CWO 3 David E. Mann

When the 108th Military Intelligence Battalion (CEWI) learned it was going to receive an influx of 97B10 Counterintelligence Assistants, the first question was "How do we use them in our operations?" Since the momentous occasion of their arrival, an internship-style rotational training cycle within the various CI and OPSEC disciplines has been formulated. In addition to rotating the new personnel through various tactical duties, on duty education in MOS related skills has also been emphasized.

Fort Huachuca's training of our 97B10 personnel only prepared them for performance of level 10 skills. There were illusions on the part of more experienced CI agents (author included) that CI assistants would arrive and be nearly as well trained at OPSEC and CI duties as a new 97B20. It was also thought that they would be able to start typing and filing between trips to the field on FTX activities. We quickly discovered that 97B10s were:

- mostly young and inexperienced, sometimes immature;
- enthusiastic about their jobs and new-found skills to the point of "bubbling over";
- sometimes disillusioned about not receiving a strategic assignment;
- highly intelligent and oriented to CI/OPSEC in a tactical environment;
- anxious to learn and then become 97B20s;
- could not type or file;
- lacked some written and spoken language skills.

With these thoughts in mind, an outline for some local training was developed.

The 108th MI Battalion (CEWI) is authorized five CI teams and an OPSEC Management and Analysis Section (OMA) in which CI slots are also authorized. Four of the CI teams are presently organized as field offices located at Bad Kreuznach (Division HQ and DISCOM), Baumholder (2d Brigade and DIVARTY), Mainz (both 1st and 4th Brigades, 4th Infantry Division (Forward) located in Weisbaden), and Mannheim (3d Brigade). Each field office falls under the jurisdiction of the Chief, OMA, during garrison, and the 108th MI Battalion (CEWI) C&J Platoon during FTX and wartime operations. OMA has several 97B20 positions unfilled due to the shortage of NCOs in that MOS, and those slots are filled by 97B10 CI assistants.

Each field office has either a senior CI warrant officer or 1st lieutenant-36A as Special Agent in Charge. Assigned to the existing 97B20 and 97B30 slots in the field offices are two or three 97B10s. OMA also has three 97B10s assigned in lieu of more senior CI personel. This mix of seasoned warrants and bright, young soldiers allows for one-on-one training programs of great value to the 97B10s. The "Old Chief" provides regular training guidance and anecdotes from personal experiences. Likewise, the OMA section has an experienced sergeant first class O5G SIGSEC specialist and two CI officers whose talents and expertise are shared with the new CI assistants.

During normal duty days, the time of the field office 97B10s is filled with a healthy mixture of soldier skills training from the host company, accompanying and assisting the CI agents in IG inspections and assistance, OPSEC surveys, liaison, and practical-type administrative tasks. For instance, a typical week of a CI assistant at a field office might look like this:

Monday to Friday: Company formation, barracks duties, PT;

Tuesday AM: Preparation for an IG inspection;

Tuesday PM: Assist in a pre-IG inspection of a brigade S2;

Wednesday AM: Office correspondence and filing;

Wednesday PM: PMCS field office vehicle (M151 1/4 ton truck and trailor);

Thursday AM: Observe subject interview;

Friday AM & PM: Prepare training—only agent report, sworn statement, and be critiqued on work by OIC of the field office.

In those cases where time and classes are available, CI assistants are also encouraged to attend 2-hour sessions at the local learning center using TEC materials, typing classes, or self-paced learning devices, to improve their MOS related skills. All 8th Infantry Division (Mechanized) learning centers ordinarily have MOS

97B20 level materials on hand, and their hours of operation are flexible so that students can review TEC materials over a long lunch hour or after duty hours. One training device of value has been the self-paced typing tutor, allowing students to learn and improve touch typing skills.

During field training exercises, the CI Teams are in direct support to the brigades or the DTOC in the case of the general support DTOC CI Team. During the last FTX, a part of REFORGER 81, CI assistants:

- conducted handheld ground and airborne photography for OPSEC reports;
- collected and sorted unclassified trash, assisting in the analysis process of those documents having OPSEC value, such as orders, notes, map overlays, and letters;
- accompanied military police investigators to collect and transport "Category A" POWs who were then interrogated by CI agents;
- assisted in those "Category A" POW interrogations, note-taking and learning questioning techniques;
- used Night Vision Devices during fixed surveillances of suspected OPFOR clandestine agent nest in the FTX maneuver area;
- observed the proper conduct of security challenges and checks by military police assigned to DTOC and CP security posts;
- assisted the CI team chief in preparation of OPSEC and CI reports.

The 97B10s working at OMA have a different mission, schedule, and learning experience; this difference is the rationale for the rotational or internship job cycle. OMA CI assistants accomplish:

- receiving and coordination of OPSEC information; posting of OPSEC vulnerabilities into the 8ID(M) "Unit OPSEC Profile" book;
- processing of security clearance requests; instructing and oversight of requesters in the correct completion of DD Form 398 and DD Form 1587; taking of fingerprints;
- edit incoming articles for the 8ID(M) "Operations Security Information Letter";
- routine liaision and coordination with the provost marshal office;
- participation in company and platoon duties, barracks activities, PT;
- PMCS assigned vehicles;
- review and summarization of incoming threat data;
- analysis of that threat data and preparation of draft threat updates;
- coordination required for maintenance of the division security clearance access roster.

Now, the key to this training program is ***rotation of duties.*** Just as a tank crewman needs to drive, load, and be a gunner, prior to commanding a tank, so must the CI assistant be familiar will all aspects of CPSEC and CI prior to further training at Fort Huachuca. In development at the 8th Infantry Division is a systematized internship program for our 97B10s. The program sets forth the following guidelines and philosophy:

- Obtain a "Be a Soldier First" attitude;
- 97B10s are assigned to learn, as an adjunct to that educational process, to perform common and MOS-specific tasks as required;
- 97B10s are not CI agents and are mostly entry-level, nonprior service personnel. They cannot be expected to possess the same educational skills and maturity of CI agents;
- 97B10s require a well-rounded, flexible program within which to learn and they must not be used for menial tasks or as the "Office Gofer"
- Periodic joint training with elements of strategic CI and OPSEC units is provided to expose them to counterintelligence skills that are not used at the tactical level for example, surveillance and strategic unit OPSEC survey participation.

Finally, some 97B10s will inevitably not measure up and will not be able to perform as counterintelligence personnel. These individuals should be impartially identified during their first year and directed into some other MOS without prejudice. This elimination process is both for the good of the Army and is fair to the service member since neither the Army nor MI can afford unqualified CI agents.

In conclusion, it should be pointed out that our CI assistants are well on their way to becoming valued assets to MI; the training job is long and time-consuming. This process of using a person for work part of the time and then training him or her the rest of the duty day has some merit. However, we here at the 108th Military Intelligence Battalion (CEWI) do not think of a 97B10 who is at the learning center as "not working," they are just working at another location for a couple of hours. When polled by this author, the most significant comment made by 97B10s was, "I really want to learn my job after all!" This program requires maximum flexibility on the part of supervisors, but gives the 97B10s ample room to grow in maturity, responsibility, and expertise. We feel strongly that 97B10s trained in this multi-disciplined, rotational job environment will be well prepared to sucessfully complete the 97B20 transition course. ★

**Cryptocorner Solution**

**SOLUTION 1:**

"This cryptogram is easy.
It shouldn't take you long.
Write only the right letters,
And never write the wrong."

**SOLUTION 2:**

"Think very hard,
Study words,
Throw ideas about.
Wear out pencils,
Work long hours,
Until you break this out."

# ELECTRONIC WARFARE IN AN OPERATIONAL ENVIRONMENT

**by 1st Lt. Gary M. Bateman**

Electronic warfare is an integral element of the AirLand Battle 2100 concept as currently announced by the U.S. Army. As a combat multiplier, electronic warfare must be considered an essential ingredient in our cooperative efforts to win the AirLand Battle of the future. The battlefield of the future will be dense with combat systems whose range, lethality, and employment capabilities surpass anything known in contemporary warfare.

Our forces, including combat support and service support elements, must be able to maneuver at the critical time and place faster than the enemy. Intelligent employment of electronic warfare, tactics and support at division and corps levels is critical to our ability to win the next war. With the increasing sophistication of both friendly and enemy electronic warfare tactical operations, maintaining command, control and communications ($C^3$) will be exceedingly difficult for either side. Electronic warfare will play a significant role in any combat scenario of the future. Our challenge is to ensure proper use of electronic warfare in training situations and in war.

**AirLand Battle and $C^3CM$**

On the modern battlefield the urgent need of our forces will be to negate the Soviet second-echelon threat. We must be able to bring our combat power to bear at the critical time and place if we hope to interdict the second-echelon threat successfully. To counter this threat, fast and accurate intelligence will be required and effective $C^3$ will be essential. Under our current comand, control, and communications countermeasures ($C^3CM$) doctrine we have four missions: destroy, disrupt, deceive, and defend. This four "d" component equation of $C^3CM$ is supported by the efforts of classic intelligence disciplines, namely: signals intelligence, human intelligence and imagery intelligence. We will physically destroy the most critical enemy command and control nodes. Next we will conduct high and very high frequency communications jamming to disrupt enemy communications. Using manipulative electronic deception and imitative electronic deception, we will deceive the enemy from our battlefield intentions, while passing him false information which will ultimately confuse his operations. Finally, we will use correct OPSEC procedures to defend friendly $C^3$ operations.

The fourfold operational concept of the AirLand Battle doctrine calls for ***initiative, depth, agility, and synchronization***. These elements are essential if a combat commander hopes to win on the modern battlefield. Our maneuver forces must be able to "see and attack in depth." In doing so, exploiting and neutralizing enemy electromagnetic systems is as important as protecting friendly systems. All of these electronic warfare functions are critical to the AirLand Battle. The efficient use of our electronic warfare assets through the proper application of doctrine and tactics is a must!

**Electronic Warfare**

Electronic warfare is an essential element of the AirLand Battle Concept. As a "combat multiplier," in support of the AirLand Battle Concept, electronic warfare listens to the enemy, locates enemy stations/emitters, disrupts enemy communications-electronics, protects our own communications-electronics, and is a factor in tactical planning. With the sucessful implementation of electronic warfare, we intend to kill/jam the ***fighters*** and collect information from the ***planners***. Our electronic warfare doctrine is divided into three subcomponents: electronic warfare support measures, electronic countermeasures, and electronic counter-countermeasures. Electronic warfare support measures and electronic countermeasures are the offensive tolls of electronic warfare that enable the Army commander to see the battlefield and stop enemy operations. Electronic counter-countermeasures are the defensive tool of electronic warfare which allow us to protect friendly $C^3$. Paramount to the application of all electronic support and electronic counter measures is one fundemental requirement: ***the satisfaction of tactical commander's operational requirements***. The tactical commander uses electronic warfare with his fire and maneuver elements to increase the effectiveness of his forces.

**COMJAM and Targeting**

The Army uses communications jamming (COMJAM) as an offensive combat measure. Along with electronic deception, COMJAM is indispensable to the combined arms effort to win the AirLand Battle. Friendly and enemy tactical operations will use both ground-based and aerial COMJAM systems on the modern battlefield. Jamming tactics are very straight-forward. Essentially jammers may be deployed in two roles: to deny or degrade enemy communications at critical times in the battle; and to support electronic warfare support measure collection efforts. Moreover, jammer attacks begin when a high priority target is detected, or a target of opportunity is found. Jamming elements must be prepared to handle some targets based on a SOP, or what is sometimes referred to as "targets of opportunity." The SOP is established

based on command priorities for jamming, and, as priorities change, so may the SOP. Also, SOP targets are those that have tactical value for the enemy, but little or no intelligence value to us. Enemy fire direction nets are an example of this and should be jammed whenever identified.

When planning our ground-based and aerial jamming operations we want to target enemy battalion-to-regiment and regiment-to-division command and control nets as much as possible. This is the key to crippling $C^2$ operations. Jamming is most effective when employed with attacking fire and maneuver elements rather than in lieu of these attacks. Jamming is situation dependent. Targets predesignated for jamming attack may not be active; or if active, they may not be dedicated. Therefore, SIGINT/EW forces at division and corps must continually search for active enemy radio nets which are both desirable and vulnerable targets. Our forces will terminate their jamming attacks when the jammer has transmitted the maximum safe period of time, when an alternate jammer has acquired the target, when the enemy ceases transmission or takes other countermeasures, or when the established control authority exercises on/off control.

### MI Battalion (CEWI)

The military intelligence battalion (CEWI) is responsible for implementing the Army's EW doctrine. Each Army division is assigned an MI battalion to provide general electronic warfare support to the division, and direct support, as required, to subordinate brigades. Specifically, the MI battalion's mission is to provide intelligence, electronic warfare and operations security support that is responsive to the commander. Significantly, in offensive and defensive operations, the MI battalion supports our combat forces by jamming enemy communications emitters. The company in the MI battalion which is the hub of the ground based ESM/ECM operations is the EW company. This company conducts all SIGINT/EW operations for the division and for all subordinate brigades. Its three platoons are controlled by the MI battalion's technical control and analysis element for detailed planning of collection and jamming missions.

### Management of Jamming Operations/Staff Relationships

This area is of critical importance in the proper execution of CONJAM support to our combat forces in the event of actual deployment to fight a war. Classically, the G3 has staff responsibility for jamming within corps and division. He and his staff integrate jamming with lethal attacks by fire and maneuver elements, prioritize enemy electronic systems to be jammed, and issue ECM mission tasking to the MI units technical control and analysis element. As the senior intelligence officer in the corps or division, the G2 provides intelligence support to the G3 in the decision process of what targets to jam and where the targets are located. The fire support element assists the G3 in the all important integration of jamming with lethal fires. This interface between the FSE and the G3 is critical to support our forces successfully as they fight, and ultimately, to destroy or disrupt enemy $C^3$ operations.

Next, elements of the MI unit provide essential support in three major areas. First, the EW section works directly for the G3 and, as part of his staff, assists him in the planning of jamming missions and the identification of jamming priorities. Second, the technical control and analysis element of the MI unit's operations center converts the G3's mission tasking into specific tasking for the deployed jamming teams. The TCAE maintains a technical data base to support all EW operations. Analysts in the TCAE research the data base to determine enemy call signs, frequencies, operating schedules, and the jamming-to-signal ratio (i.e., the power needed to degrade the victim receiver effectively). This information is passed to deployed jamming teams in the form of an ECM tasking message. Third, the COMJAM systems organic to the MI unit execute the actual jamming missions.

Regarding COMJAM operations, it is significant to emphasize that both friendly and enemy EW tactical operations will maximize the use of ground-based and aerial ECM systems on the modern battlefield. ECM will support covering force operations in the defense through the selective employment of powerful, mobile communications jamming systems. In the main battle area, support of defensive operations will be accomplished by SOPs and preplanned jamming. Jamming elements must be prepared to react at a moments notice to suspected enemy activity while either in the covering force or main battle area. Targeting decisions made concerning enemy command and control nodes by COMJAM teams in a coordinated manner with fire support elements and the TCAE are: whether or not to jam; to jam and destroy simultaneously; to destroy; to deceive; to jam and exploit; or to monitor or exploit.

### Conclusion

The Army's intelligent application of EW in an operational environment is vital. EW is an indispensable element of combat power and will play an ever increasing role in the Army's successful execution of the $C^3CM$ and AirLand Battle 2100 concepts. Proper use of EW tactics will enable our division and corps commanders to better see the battlefield as they plan to fight the enemy. Electronic warfare will aid the efforts of our fire and maneuver forces by developing and exploiting critical enemy $C^2$ targets, jamming enemy communications links (especially at the regimental level), and maintaining friendly communications. The successful implementation of EW on the modern battlefield will certainly impact on our ability to win—regardless of whether or not our forces are operating in a defensive or offensive posture. Our challenge is to provide field commanders with the necessary EW support to ensure the ultimate success of their mission. ★

---

*1st Lt. Gary M. Bateman holds a BA degree in History from Wichita State University and an MPA degree in Public Administration from from Golden Gate University. He has served in the Army's tactical SIGINT/EW field for over seven years. Bateman received his commission in 1981 from OCS and is a graduate of MIOBC, 37A, and 35A intelligence courses. He currently serves as tactical electronic warfare instructor for the 37A course with the SIGINT/EW Branch, Department of Tactics, Intelligence, and Military Science at Fort Huachuca, Arizona.*

# The Tactical Army and Counterintelligence

## Why it is important and how it can be used by the commander

**Counterintelligence personnel must be professional and aggressive in their efforts to strengthen the tactical unit into an effective fighting force by helping to educate the commander in how to use the CI element.**

by CWO 2 Herbert G. Taylor Jr.

"All military personnel are potential sources of information and action that may aid the enemy to gain knowledge of the location, strength, composition, equipment, plans for operations, and status of supply and morale of our forces and those of our allies. That any harmful action or disclosure of information by an American soldier might be completely unintentional will not lessen the enemy's gain. Intensive enemy programs of espionage, sabotage, and subversion are constantly in operation. Propaganda and demonstrations designed to damage morale and divide allies often masquerade as honest, patriotic criticism. The heritage of the American soldier allows for unprecedented freedom of speech and action. This freedom tends to work against the maintenance of military security, as does a friendliness and an informality of manner during the performance of military duty. Methods employed by enemy intelligence organizations are so insidious as to be unthinkable to the American soldier unless training and constant reminders create and maintain an acute awarness of enemy intentions, capabilities and methods of operations."[1]

The problem starts with the Soviet Union's ability to collect information about the United States. Soviet collection is designed to paralyze U.S. defenses and to rob the freedom on which the United States was founded. The problem is compounded through the inability of some believers to convince nonbelievers that the Soviet Union represents a viable collection threat and that countermeasures need to be implemented immediately.

"The KGB is the all-powerful intelligence organization of the Soviet Union. Second only to the communist party, the KGB is responsible for Soviet espionage throughout the world. From bases in Canada, Mex-

*CWO 2 Herbert G. Taylor was appointed a warrant officer in August 1978. He is a graduate of Utah State University, as well as the MI Warrant Officer Advanced Course and Senior Course. Presently the Training Officer for B Company, 519th MI Battalion, Fort Bragg, N.C., Taylor has previously served in Vietnam with the 101st MI Company and Italy with the 66th and 650th MI Groups.*

ico, and the U.S., the KGB has operated illegal espionage nets. From the Soviet embassy in Washington D.C., and the United Nations, legal KGB agents operate with relative impunity, many enjoying the privilege of diplomatic immunity."[2]

It is clear that Soviet espionage is and will continue to be a threat that the Army must reckon with. CI has the expertise to counter this threat within the tactical command and to contribute to the support of the commander on the battlefield. The fact that CI has the ability to help the tactical commander make a more effective fighting force is merely a matter of command education. To be truly effective, tactical units must guard the disclosure of their own strengths, while at the same time seek knowledge about the enemy.

Counterintelligence possesses many of the necessary assets to lessen the Soviet espionage threat and help commanders construct a more enemy-oriented fighting force. The commander who has the best intelligence of the battlefield and uses it to his advantage has the decided edge in the balance of combat power. CI capabilities range from classified document protection, both in garrison and on the battlefield, to the construction of a CI estimate. This estimate aids the commander in evaluating the enemy's intelligence, sabotage, and subversive capabilities, and in determining the relative probability of enemy adoption of such tactics. Tactical counterintelligence personnel are trained to see through the eyes of an enemy commander. They, in effect, change places with the opposition in an effort to gain knowledge about enemy strengths and weaknesses. In this manner, CI can determine friendly unit vulnerabilities. This threat analysis can prove invaluable in predicting potential security violations and recommending corrective changes.

CI maintains valuable human resources, which provide a wealth of knowledge of enemy signatures, patterns and profiles. With this information, the commander can predict unfriendly actions before they occur. The commander should remember that when cloud cover, adverse weather, or terrain features, hamper electronic methods for collecting information, human assets can obtain the information that is vital to the unit's survival and effectiveness.

"Although electronics can locate enemy units and trace their movements, electronics cannot determine what the thoughts of an enemy commander are. Human intelligence can determine when, where, and how an attack can and will take place."[3]

The AirLand Battle doctrine has placed an enormous task on tactical CI disciplines. The commander needs enemy routes of advance, movement tables, and relative target values, as early as 96 hours before the enemy will engage friendly forces along the forward line of own troops.

CI is perhaps the least understood discipline within the intelligence arena. The commander has an extremely valuable asset in CI and must learn to equate its usefulness with the fundamental principles of war: security and surprise.

"To achieve and maintain these principles requires that the friendly commander be able to deny and control the enemy's ability to collect intelligence. The tools available to the commander to do this job are tactical CI and operations security. Tactical CI and operations security are multipliers of combat power. Tactical CI challenges the hostile collection effort while operations security protects and identifies friendly vulnerabilities."[4]

Commanders are always concerned about their mission and those specific disciplines which are necessary to accomplish that mission. This attitude must be expected of a commander and is not wrong in basic context. However, during the preparation phase of an impending battle, bits and pieces of important information are sloughed off and forgotten. Forgotten to the commander, perhaps, but not to the enemy. Through the collection of many forgotten pieces of information, the enemy is able to construct an important picture of friendly capabilities and strengths. The answer to this dilemma is operations security. The main object of operations security is to determine the essential elements of friendly information and ensure they remain unknown to the opposition. The commander will soon realize that operations security must be continuous, concurrent, and coordinated with all operational planning during periods of static and tension, as well as, combat. We do in combat what we practice in peacetime. Operations security can be effective in any environment, but their concepts need rehearsal in peacetime, so that in times of conflict their practices are second nature. When combat starts, time becomes a critical factor, and the bulk of CI becomes driven by events.

The key to proper CI use is the tactical commander. However, before the commander can influence any situation for the good, there must be the "know how." Without that basic knowledge, there can be no positive direction. CI personnel must be professional and aggressive in their efforts to guide that tactical commander and the unit towards the ultimate goal of an effective fighting force. Assignment, at the tactical level, provides a vehicle and a challenge for CI personnel to "educate the commander." Tactical CI personnel need only sell trust in their product for the commander to be a full-time subscriber. As soon as the commander realizes the worth of CI assets, trust and compliance will follow.

The first and foremost task necessary in directing the CI effort, in a unit, is a viable security education program. Few tactical units possess an acceptable security education program. They might have the documents and Army regulations necessary to start one, but the enthusiasm is usually lacking. The driving force, in almost all cases, must be organic CI personnel within the unit or the intelligence staff element. A good security education program will place emphasis in critical areas: subversion and espionage directed against the U.S. Army, document security, hostile threat analysis, sensitive elements of the unit that need extra protection, operations security procedures and terrorism analysis and support. Awareness and adherence to these principles will strengthen unit fighting capability and effectiveness, as well as make the commander aware of CI assets. Through a good security education program the tactical commander will realize that CI can play a vital role in the preparation of troops to meet the enemy.

Once the unit security officer has secured the commander's trust in CI, he can seek out specialized support from a CI field or resident office. These personnel have the ability to tailor special security programs unique to a specific unit. Most tactical units can benefit in general from routine security practices, but some units have special missions that require detailed consideration. An example might be in units capable of nuclear weapons delivery. Units in this category are faced with sensitive personnel problems and nuclear movement security that is unique to other parts of the military. CI can and should work with such a commander in preparation for specific needs.

Good security was never meant to be convenient. It takes a great deal of discipline and sacrifice, as well as a

commander who has the "right education."

Cooperation has always been important in any big business and the Army is no exception. Once the commander has been sold on the benefits of CI and has allowed these programs to proceed, the situation still balances between the commander and the operating security force, where an unbreakable mutual trust must exist. The security element must do everything in their power to support the commander and to keep him informed of all happening and potential problems. Security is a service that is provided to the commander. He may accept or reject, in whole or part, many of the recommendations given. This is a common grievance and the security element must not become disheartened at the reversal of some decisions. Based on experience, the security element will know whether or not to push above the commander's authority. This is a delicate decision and must be handled diplomatically, to avoid alienation.

Liaison is an important practice in establishing cooperation with the commander. The CI element must make frequent contact and try to understand the commander's needs. CI activity is worthless unless it is directed to fulfilling the needs of the user.

CI skills and programs require practical application to maintain high standards of competence and understanding. CI elements and unit security personnel must seek areas of opportunity (such as joint exercises) to practice the effectiveness of their trade. Just as a well-tuned engine requires stress and strain to prove its worth, so does an organization need practice to temper its skills.

Tactical unit security personnel must continually monitor their areas of responsibility in an effort to upgrade existing programs. They must also check unit personnel concerning adherence to security practices. No program can be effective with only partial involvement.

Tactical units do not always continue with the same mission year after year. Security elements have a responsibility to reassess unit direction and attitude, at least annually. This will provide for changes in threat assessment and retailoring of security needs. Tactical units are never static. Their missions tend to be very dynamic in nature and, therefore, dictate that security support be the same. Tactical counterintelligence has much to offer the commander, whether it be in peace or war. CI broadens the tactical unit in both depth and effectiveness through education of the commander.

"Two factors have led directly to the increased importance of Army tactical intelligence: (1) The U.S. does not hold the strong military advantage that it did in World War II. The U.S.S.R. is much stronger and more threatening. We do not enjoy superiority in numbers. Therefore, we will have to recognize that accurate and timely intelligence can and must compensate for much of the imbalance in size of the opposing forces. (2) The qualitative advancements in weapons systems, particularly their lethality and mobility, have placed a premium on advance knowledge of enemy capabilities, deployments, and intentions."[5]

The need for more and better counterintelligence support to the tactical unit has been made quite obvious. Therefore, it is essential to national security that the commander be educated towards CI worth. Without the added assets that CI can provide to a commander's combat effectiveness, victory in the next conflict might be in doubt.★

**FOOTNOTES**

1. Frank L. Brown, "Critical Combat Performances, Knowledges, and Skills Required of the Infantry Rifle Squad Leader, Counterintelligence." HUMRRO Division No. 4 (Infantry)-The George Washington University Human Resources Research Office Operating Under Contract with DA. (December 1968) pg. 1.
2. Merritt M. Smith, Capt., U.S. Army, "The KGB vs The USA," Research Paper for Class C-22-3. (11 September 1978) pg. 12.
3. Stephen L. Burkart, Sgt., U.S. Army, Personal Interview Concerning: "Tactical Counterintelligence and the Commander" conducted at Fort Huachuca, Ariz., August 1982.
4. Ibid.
5. Robert J. Covalucci, Lt. Col., U.S. Army, "ACSI Viewpoint-An OACSI Perspective-Tactical Intelligence," **Military Intelligence** (April-June 1982) pg. 37.

## CHANGES of ADDRESS

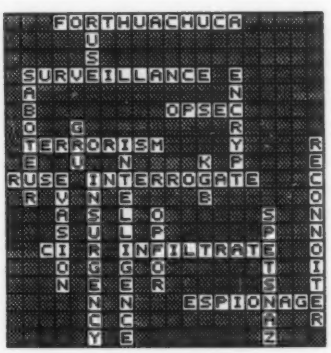
Attention subscribers! The **Military Intelligence** offices are still receiving changes of address for your subscriptions. The Superintendent of Documents, U.S. Government Printing Office is handing the subscriptions to **Military Intelligence**, and is the place to send your changes of address. All changes of address sent to Fort Huachuca will be forwarded, but slow service may be the result.

**New subscriptions** continue to trickle into the Fort Huachuca mailbox and are returned to sender with a form letter of explaination. Please, send it to the G.P.O.! We continue to receive subscription forms that are two, three, and sometimes nine years old. Pass the word to check the most recent issue for rates and the proper address to send checks and money orders.

**Official distribution** to units is **not** handled by the G.P.O. Send requests for official distribution to the **Military Intelligence** offices at Fort Huachuca.

**Back issues** are available on a very limited basis for selected organizations only. Private individuals will have to search elsewhere to find back issues of the magazine. Sorry, but we're down to only two copies of some back issues and are forbidden to sell any extra issues that we do have.

For more information, see the fine print at the bottom of this issue's table of contents.



# USAICS Notes

## General Weinstein's Second Star

Brig. Gen. Sidney T. Weinstein, commander of the U.S. Army Intelligence Center and School, pinned on his second star in a "frocking" ceremony, Nov. 25, 1983 at Fort Huachuca.

Presiding over the ceremony was Lt. Gen. Carl E. Vuono, deputy commander of the U.S. Army's Training and Doctrine Command.

The ceremony was held in front of Riley Barracks, the Intelligence Center and School Headquarters.

Weinstein was commissioned a second lieutenant of infantry in 1956, following his graduation from the United States Military Academy at West Point. In 1962, he transferred from infantry to military intelligence. He has served in military intelligence positions in Central and South America, Vietnam and Europe.

His assignments include: command of the 2d Military Intelligence Battalion in Europe and the 525th Military Intelligence Group at Fort Bragg, N.C. He also served as the Assistant Chief of Staff for Intelligence for the XVIII Airborne Corps, the executive officer to the Army Assistant Chief of Staff for Intelligence, and the deputy commander of the Army Intelligence and Security Command. He has commanded the U.S. Army Intelligence Center and School since August 1982.

Weinstein's decorations and awards include the Legion of Merit, the Bronze Star, the Meritorious Service Medal, two Air Medals and the Army Commendation Medal. Also, he has been awarded the Master Parachutist Badge, the Pathfinder Badge and the General Staff Identification Badge.

Weinstein now resides at Fort Huachuca, Ariz. with his wife, Pauline, and son, Michael, who attends high school in Sierra Vista, Ariz. He also has two daughters, Halee and Mila, who both attend college.

**Maj. Gen. Sidney T. Weinstein, commander of the Intelligence Center and School, receives his second star from his son, Michael, and Lt. Gen. Carl E. Vouno, deputy commander of TRADOC, during "frocking" ceremonies at Fort Huachuca.**

**(photo by PFC Ron Hill)**

**Weinstein gets a handshake from one of the younger attendees of the "frocking" ceremony held at Fort Huachuca, Ariz.**

**(photo by 2nd Lt. Kevin Austra)**

# EICHELBERGER'S PROMOTION

☆ ★ ★ ★ ★ ★ ★

Brig. Gen. Charles B. Eichelberger, Deputy Commander of the U.S. Army Intelligence Center and School, Fort Huachuca, Arizona, pinned on his first star January 24, 1984 in a ceremony in front of Riley Barracks. Eichelberger has been serving as USAICS' Deputy Commander since October 1982.

He was born in LaGrange, Ga., November 19, 1934 and entered the service in September 1955 as an enlisted man. He was commissioned a second lieutenant after graduating from the Infantry Officer's Candidate School in 1957.

Following training at the Infantry Center, Eichelberger was assigned as a platoon leader and watch commander, 5th U.S. Army Security Agency Field Station, Hawaii. He was assigned to the 317th U.S. Army Security Agency Battalion, Ft. Bragg, N.C., in 1960. During this tour, he commanded the first Army Security Agency Direct Support Airborne Company, supporting the 82nd Airborne Division.

In 1962, Eichelberger was assigned to Vietnam for duty as the intelligence operations officer of the 3rd Radio Research Unit. He returned to the 317th ASA Battalion and served as the operations officer, and in 1965 was the operations officer for combat operations in the Dominican Republic.

In 1966, he served as an intelligence analyst with Deputy Chief of Staff for Intelligence Support Indication Center assigned to U.S. forces Korea and the 8th U.S. Army.

Eichelberger attended the Command and General Staff College, graduating in 1969. At this time, he was assigned as chief and instructor for the Crypotologic Committee of the Advanced Course Department at the U.S. Army Intelligence School at Fort Holibird, Md.

From July 1970 until June 1973, Eichelberger commanded the 313th U.S. Army Security Agency Battalion (Airborne). He established and commanded the first Cryptologic Support Group assigned in support of U.S. Army Pacific until July 1975, at which time he attended the Army War College, graduating in June 1976.

After graduation, he served as deputy director for intelligence, Intelligence Center, Pacific, until January 1977. At this time, he was assigned to Operations, CINPAC as deputy direc-

**Brig. Gen. Charles B. Eichelberger, deputy commander of the Intelligence Center and School, receives his first star from Maj. Gen. Sidney T. Weinstein, commander of USAICS, and wife Jackie Eichelberger at a ceremony in front of Riley Barracks. (Photo by PFC Ron Hill)**

**SUBSCRIPTION ORDER FORM**

Deposit Account Number

| | | | | | | | – | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |

*Enclosed find $_____ (check or money order), or charge to my Superintendent of Documents Deposit Account Number shown above.*

*Your Order Number*

*Please send the subscription(s) I have listed to the address shown at the bottom of this form.*

MAIL ORDER FORM TO:
Superintendent of Documents
U.S. Government Printing Office
Washington, D.C. 20402

| FOR OFFICE USE ONLY | |
|---|---|
| Quantity | Charges |
| ..... Enclosed | |
| ..... To be mailed | |
| ..... Subscriptions | |
| Postage | |
| Foreign handling | |
| MMOB | |
| OPNR | |
| ..... UPNS | |
| ..... Discount | |
| ..... Refund | |

master charge

VISA

Credit Card Orders Only
Total charges $_____. Fill in the boxes below:

Credit Card No.

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | |

Expiration Date Month/Year

| | | | |
|---|---|---|---|
| | | | |

Master Charge Interbank No.

| | | | |
|---|---|---|---|
| | | | |

*NOTE: Complete top address portion if different from that at the bottom.*

Name _____

Street address _____

City and State _____ ZIP Code _____

| SYMBOL | TITLE | PRICE |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

NAME—FIRST, LAST

COMPANY NAME OR ADDITIONAL ADDRESS LINE

STREET ADDRESS

CITY | STATE | ZIP CODE

(or) COUNTRY

**PLEASE PRINT**

GPO Form 3625
(3-79)

## ORDERING INFORMATION

The prices of all U.S. Government publications sold by the Superintendent of Documents are established by the Public Printer in accordance with Title 44 of the United States Code. Prices are subject to change and the prices charged on your order will be those in effect at the time your order is processed. As it is not feasible to manually correct the prices in the publications affected by price changes, the prices charged on your order may differ from those printed in the publications. Although the issuing agencies generally know about price changes, some agencies inadvertently continue to publish announcements, order forms, and catalogs which contain erroneous prices. Frequently, the news media publishes articles with erroneous or outdated prices.

---

Subscriptions are accepted for 1 year only unless otherwise specified. Subscribers will be notified prior to the expiration of their subscription in ample time to effect a continuity of service.

---

Orders to foreign countries require a special handling charge. The charge is approximately one-fourth of the current selling price of the subscription service ordered and is included in the Foreign subscriptions price. This charge is to cover the special handling required to comply with the customs and international mailing regulations.

---

The average processing time for new subscriptions takes 2 to 6 weeks plus mailing time. The large volume of mail we receive each day makes it virtually impossible to locate a subscription order until it has been entered into our computer. Please take this into consideration before making inquiry concerning periodicals and subscription services in compliance with Paragraph 1708 of Title 44, U.S. Code. Effective January 1, 1974, for orders entered or services commencing after that date, the discount policy is:

A discount of 25 percent will be allowed to bookdealers when the publications, pamphlets, periodicals or subscription services are mailed, delivered or forwarded to the dealer's normal place of business.

A discount of 25 percent will be allowed to quantity purchasers (100 or more copies of a single publication, pamphlet, periodical or subscription service) when mailed to a single address.

No discounts will be allowed when the publication, pamphlet, periodical, or subscription service is mailed to a third party (unless in quantities of 100 or more), or on those periodicals or subscription services which fall into a special pricing category.

### WHERE TO ORDER

Orders should be addressed to the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. In addition to your address, please include the title and price of the subscription together with the subscription symbol that appears in the brackets following the price. For example: **[COBD]** identifies the Commerce Business Daily.

### HOW TO REMIT

The rules of this Office require that remittance be made in advance of shipment of your subscription. Your check or money order should be made payable to the Superintendent of Documents. Foreign money and postage stamps are not acceptable. Remittances from foreign countries should be made by international money order payable to the Superintendent or by draft on an American or Canadian bank. UNESCO Coupons are also acceptable from foreign countries. For the convenience of customers who make frequent purchases, a prepaid Deposit Account may be opened by remitting $50 or more. Upon receipt in this Office,you will be assigned a special Deposit Account Number against which future orders may be placed without making individual remittances or first obtaining quotations. It is suggested that a balance sufficient to cover 3 months' purchases be maintained to avoid the necessity of frequent deposits. Orders may also be charged to your Master Charge or VISA account. Please include your card number, date of expiration, and interbank number *(Master Charge only).*

GPO: O-283-641

tor for operations, and later as the deputy chief, Command and Control Division, with an additional duty as the CINCPAC chairman of the C-4 (Command, Control, Communications, and Computers) Work Group.

In June 1978, Eichelberger assumed command of the Intelligence and Security Command's field station in Berlin. He returned from this group-level command in August 1980, at which time, he became the division chief for the Intelligence, Surveillance, Target Acquisition, and Electronic Warfare Division of the Requirements Directorate, ODCSOPS, DA.

Eichelberger's decorations and awards include four Legions of Merit, both a Joint and Army Meritorious Service Medal, and two Army Commendation Medals. Additionally, he holds the Vietnamese Cross of Gallantry with Palm, and both the Army and Air Force Unit Commendation Awards. He has been awarded the Master Parachutist Badge.

Eichelberger and his wife Jackie reside at Fort Huachuca and have two daughters, Susan and Terrie.

## Have a Good Field SOP? SHARE IT!

*The ongoing expansion of the military intelligence training and evaluation program, which assists you with MI unit training, requires your input. Unclassified and classified SOPs of MI battalions and companies are sought as baseline information for standardizing unit training products within the Army Training and Evaluation Program, which encompasses the training and evaluation outlines, the MI Army unit test, MI drills, and the technical support package. Our efforts will be directed toward producing a standard unit reference and we intend to cite those units which provide input.*

*Send in your field SOPs. If your SOP requires special handling, forward through ARFCOS channels to Commander, USASSD (SSO), Fort Huachuca, Ariz. 85613. Other materials may be forwarded to: Commander, USAICS, ATTN: ATSI-TD-CT, Fort Huachuca, Ariz. 85613. Or, if you prefer to call, reach the MI unit trainers on AUTOVON 897-5769/3207.*

# Department of Defense Strategic Debriefer Course

For years, commanders of units with strategic debriefing missions have expressed concern over the lack of debriefer training. The only training Army and Marine interrogators received was the basic tactical interrogation course taught at Fort Huachuca, Ariz., and language training at the Defense Language Institute at Monterey, Calif. Air Force and Navy personnel do not have a basic interrogation course. Personnel of all services had to learn the skills and background required for strategic debriefing on the job. The learning process averaged eight months.

In 1981, the Defense Intelligence Agency conducted and validated a study stating a need for debriefer training. In June of 1982, the Army agreed to accept executive agency responsibility for a strategic debriefer course. Between June and September 1982, a Memorandum of Agreement was written and signed by DIA and the senior intelligence officers of the Army, Air Force, Navy and Marine Corps. The Army Intelligence Center and School was designated as the proponent for development and administration of the course. Instruction began August 1, 1983.

The course is intended to be assignment oriented. Students should be on orders to or already be assigned to a strategic debriefing activity. The MI Proponency Office at USAICS is working with the Soldier Support Facility to identify and justify the assignment of an additional skill identifier or special skill identifier for active Army graduates of the course.

The strategic debriefer course is six weeks long with a maximum and optimum class size of 12 students. Class composition is usually eight Army, two Air Force and two Marines, with Army slots reduced when Navy or other intelligence agency students attend. Student ranks are immaterial. Two SDCs were conducted during Fiscal Year 1983 and seven are scheduled for Fiscal Year 1984. Eight interations per year are projected for Fiscal Year 1985 and beyond.

The overall objective of the SDC is to reduce the on the job learning time by six months. To accomplish this, the program of instruction includes overviews of the strategic intelligence community, advanced training in neurolinguistic programming rapport building techniques, methods of dealing with various personnel being debriefed, and report writing.

Each student takes part in an intensive nine-day debriefing practical exercise. During this phase, students debrief role players using real world scenarios and are required ot write appropriate reports. The entire exercise is designed to be stressful as well as realistic. The students normally spend four to six hours each night writing reports and preparing for the next day's debriefing. The debriefings are tailored to the specific needs of each student. In addition, the course features an elective program which allows students to select their own special training.

For additional information, contact the Chief, Exploitation Division, Autovon 879-5272/3837.

# USAISD Notes

## Electronic Warfare Operations Course

A new concept for training of tactical electronic warfare personnel is being developed at USAISD. The USAISD training has been a mixture of some tactical and some strategic instruction. Until now, the training of 98C and 98G personnel has been skill level two tasks before going to their initial unit. The actual equipment "hands-on" for these personnel has been a hit-or-miss affair. Few 98G personnel have actually attended the Electronic Countermeasures Equipment Operators course (K3) for hands-on training before going to a tactical assignment.

Thanks to a decision on responsibilities for executive agent training, plus input from the field, USAISD training for 98C and 98G personnel will concentrate on tactical operations. Goodfellow Air Force Base will teach the strategically-oriented skills. Those individuals going to tactical assignments will receive further training at USAISD in the EW Operations Course. Additionally, those personnel going to an initial tactical assignment (up through E7) will also attend the EWOC.

The EWOC will be phased into existence beginning in March 1984. The first phase will be approximately six weeks long with additional training added as new systems are available up to an eight week maximum length. The purpose of the EWOC is to produce a tactical EW soldier who is a proficient weapons system crewman in his technical job and his common soldier tasks. Initially the EWOC will train the EW soldier on the AN/TRQ-32 and AN/TRQ-30 radio receiving sets and the AN/TLQ-15, AN/TLQ-17, and AN/GLQ-3B countermeasures sets. Besides receiving hands-on qualification on this equipment, and the additional skill indicator K3, the student will also learn EW doctrine, EW targeting, and application of many common soldier tasks to the duties of an EW equipment crew. The tactical commander will receive an EW soldier who is better able to step right in and pull his share of the load on the battlefield.

The first personnel to attend the EWOC will be 98G's and 05H's headed to tactical assignments. When the strategic training for 98C personnel is totally transferred to GAGB, the 98C training at USAISD will also become a part of the EWOC. The 98C will focus on low-level voice communications and meeting the tactical commanders intelligence needs as well as trageting EW assets. The Technical Control and Analysis Center will become a major part of the 98C training when it arrives at USAISD in the autumn of 1985.

## TACJAM

Two AN/MLQ-34 (TACJAM) Systems recently arrived at the U.S. Army Intelligence School, Fort Devens. The TACJAM System is a high powered communications jamming system, built by GTE, Sylvania of Mountainview, Calif. It is designed to deny, deceive, or disrupt enemy communications in a tactical environment. The computer assisted system stores data on up to nine primary targets and nine alternate targets, and will protect up to 20 frequencies or frequency bands from jamming. Operations are performed automatically with operator assistance or with direct operator control.

The electronics are installed in an S-595 shelter which is mounted on a modified M-548 (SM-1015) tracked cargo carrier. A pneumatically operated telescoping log periodic antenna and electrically driven ground rod driver aids the operator in operational set-up, mission performance, and redeployment in an extremely short period of time. A liquid-to-air heat exchanger dissipates heat from the internal transmitters, and a 36,000 BTU air-conditioner maintains the ambient temperature for the remainder of the internal electronics equipment, as well as providing reasonable comfort for the operator.

The U.S. Army Operational Test and Evaluation Agency recently completed a 30-day test of the system at Fort Stewart, Ga., utilizing troops from the 24th Infantry Division. By placing the system in the hands of Army operator (MOS 98G) and maintenance (MOS 33S) personnel trained by the contractor, OTEA evaluated the capabilities of soldiers to employ the system in support of tactical commanders.

The two systems will be used at USAISD to train crew members and maintenance personnel. Operator training is to be integrated into the Electronic Countermeasures Operator Course while maintenance training will be integrated into the new Tactical Equipment Repairer Course (33T) currently being developed. With additional procurement for further TACJAM systems under contract, an increased load will be placed on USAISD to maintain a constant output of operator and maintenance personnel for an extensive period of time. Training students to perform intelligence tasks in support of the tactical/strategic commander is the mission of USAISD and use of the TACJAM System will help us keep our soldiers the best qualified in the world.

## 98C/98G Combined FTX

"During the third week of your course you will be going to the field." These words, spoken by their instructor during the introduction to their class, probably caused a great deal of apprehension and misgivings to the 98G voice intercept operators, and 98G analysts, who were preparing to receive the last courses of instruction before reporting to their field unit. Many of these student soldiers' only experience with field operations had been in Basic Training and that was almost a year-and-a-half in the past. Questions assailed the instructors as the time before leaving grew shorter.

The COMINT Branch, EW/C&S Department, Deputy Assistant Commandant for Training, U.S. Army Intelligence School, Fort Devens, initiated field training exercises over a year ago to provide functional course students (those who have completed

their MOS training) with reinforcement of the training received in BCT and AIT in field survival techniques, site prep, teardown and operation of tactical SIGINT/EW equipment, and the function, operation and deployment of a Collection and Jamming platoon in the field. Although the students had received almost all of their individual skill training, the FTX teaches them to operate as a team—a team that not only has to survive under combat conditions, but also must perform its mission of supporting the brigade and division tactical commanders with as rapid and accurate a picture of the battlefield as possible.

Students of the F232-F3, 005-83 Army Unique Analysis Course and F12-501/502 and 503 Voice Interceptor classes were briefed on Operations Order 003 that would cause deployment of a Collection and Jamming platoon. The following Monday, both classes drew TA-50 equipment and loaded vehicles in preparation for deployment. The platoon consisted of two collection teams with the TRQ-30 and TSQ-114 TRAILBLAZER, two jamming teams with the TLQ-17 and GLQ-3B and a Traffic Analysis Team. Students and instructors were prepared to support the Notional 181st Infantry Brigade, as the EW/C&S Department C&J platoon.

Under the exercise scenario spelled out in Operations Order 003-83, the C&J platoon would be providing Electronic Countermeasures OPFOR in support of the 181st Infantry Brigade which was facing a Motorized Rifle Division which was rapidly approaching from the north of Fort Devens along Route 225 and the Nashua River. Because of reports of scattered enemy reconnaissance teams, the platoon was divided up into an advance party to be lifted into the area to secure the position, while the balance of the platoon followed with the vehicles and equipment.

At 5 a.m., the 39 students were alerted and moved through the halls of student company, 2nd Battalion, Second Schoo! Brigade, Fort Devens. Nervous anticipation filled otherwise sleepy eyes as the students donned their gear and filtered out into the early morning sun. Outside the building, instructors checked the students' LC-1 packs and load bearing equipment. Many of the instructors had been up since 3 a.m., preparing their own gear. All personnel double-checked to insure they had their ID cards and dog tags, prerequisites for flying on Army helicopters. M16 rifles and magazines were issued.

**98G, intercept operator and 98C, analyst students board a helicopter furnished by HQ's, CMD, USAG, Ft. Devens.**

At 7:30 a.m., the first of three sticks of the Traffic and Analysis team, with SSgt. Bruce K. Bickel, a 98C instructor, and led by the C&J Platoon Sergeant, SSgt. Yandell; lifted off from the Pickup Zone at Rogers Field. For most, this was their first ride in a UH-1 Huey helicopter. The Landing Zone was reportedly hot. It was their job to secure and hold the LZ until the remaining elements of the T&A Team arrived. At 7:50 a.m., SFC Richard Hanspire and SSgt. Terry Tibbs, 98G/98C site commander and assistant site commander respectively, received the call, "Zulu One-Four, this is Sierra Three-Six, Lima Zulu secure. We are moving out to secure site one, over." The T&A team moved to secure the site which was to be used by the C&J platoon, one-and-a-half miles northwest of the LZ. The platoon sergeant or student NCOIC then had to deploy the rest of the C&J platoon. Twenty minutes into the deployment, another call was heard on the radio. "Zulu One-Four, this is Sierra Three-Six, the site is secure, over."

The remainder of the team had completed vehicle loading, and with TRAILBLAZER and the TQO-30 team, deployed to the base site, arriving at 9 a.m., to start setting up. The TRAILBLAZER and TRQ-30 teams deployed approximately 300 yards west of the base site and began to initiate training in system operations. Sp4 Kerr,, 505th ASA, a member of the Reserves, trained his team in the operation of the TRQ-30 to the point where they could operate the entire system themselves on the next day. SSgt. Harris, the TRAILBLAZER instructor, had his team camouflaged and up within two hours. During the afternoon, the team erected the H-Adock antenna to 26 feet. Both teams were ready to begin operations. Communications were achieved with the base site both by radio and field telephone. Meanwhile, the T&A Team and the jamming teams had been establishing the base site and their bivouac area. They erected a GP medium tent for SCIF operations and GP small tents, which would serve as an access point for the USAISD MP platoon contingent and student SCIF guards, to control access. After three strands of concertina wire had been emplaced to prevent unauthorized SCIF access, all teams began training in perimeter defense; security; and light, noise and litter discipline. The base site and mess area were fully established by 4:30 p.m. All personnel were ready for nightfall.

Perimeter defense points and guard

98G/98C students under simulated ambush attack.

posts were now assigned and manned. The guard posts communicated with the operations area by field phone, and roving guard by radio.

Intelligence reports indicated that OPFOR vehicular and foot patrols were in the area. At 9 p.m., several shots were fired from an unknown enemy force. Radios and field phones buzzed with activity. Uncertain at first, the students pin-pointed the assaulted area. Guard Post Bravo and the collection teams had been fired on. A reaction force rushed to the rescue, only to meet heavy small arms fire. A student crouched low in the brush by a small tree, peering into the darkness. One tree branch, pointing in his direction puzzled him. Panic instantly followed realization. He began to move, but too late. The "tree" spoke in a calm voice, barely hinting of its lethality, "Make one move and you are a dead man!" Lessons are learned the hard way in combat.

Thirty minutes later, the "aggressors" had been repelled. The action was critiqued to point out both right and wrong moves. All the students had learned something that night, one particularly so. Full operations resumed. Those not on duty headed toward the bivouac area. Sack time is a rare commodity in field training and the students had been told to get all the sleep they could. Five a.m. came very early. That day, the students were given more instruction on site security and perimeter defense. They also received hands-on training on operation of the 10 KW generator and Preventive Maintenance Checks and Services on the M15A1 jeep. Instructors from ECM Branch, under the direction of SFC McMeeken, arrived on site with the TLQ-17 and GLQ-3B jammers. Their teams moved out to the sites and commenced training. By the end of the day, SSgts. Harrington, McRae and Salsbury had both teams performing set up and teardown of these systems to ARTEP standards. During the day, the TRAILBLAZER team had erected its data link antenna and continued training on PMCS and perimeter security. The TRQ-30 had deployed after breakfast on site reconnaissance, and by 10:30 a.m. had reestablished themselves on the top of an old building about 500 meters southeast of the base site.

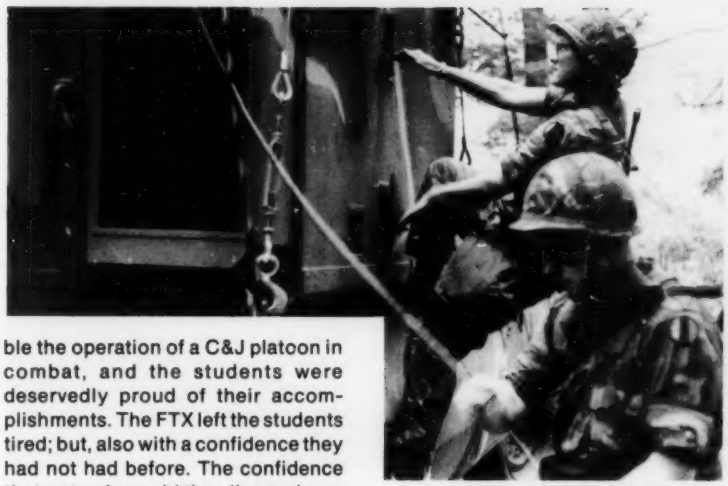
Sgt. Gipson, the T&A team leader and assistant platoon sergeant, had organized her personnel into sections and was prepared to start operations. At 7 p.m., upon receipt of orders from the site commander, Gipson issued two ESM Tasking Messages to TRAILBLAZER and TRQ-30 to begin operations against the notional enemy force which had deployed along Route 225 about 10 kilometers to the north. The OPFOR was expected to begin a full assault on the supported brigade early the next day. Both collection teams immediately started full operations in a simulated combat environment and continued them through the night. The platoon successfully repelled an assault by an aggressor foot patrol (which used small arms and chemicals) at 11 p.m., while the mission continued.

At 5:30 a.m. the jamming teams redeployed, and upon receipt of ECM TAMs 001 and 002, commenced missions against the OPFOR advance guard and artillery. By 7:30 a.m., the platoon was ordered to tear down and

**98G/98C students prepare the AN/TSQ-114, TRAILBLAZER Special Purpose Detecting System for operations.**

redeploy to prevent them from being overrun. While the jamming and collection teams provided security, the T&A team commenced teardown. By 8:15 a.m., the C&J teams were tearing down. At 8:35 a.m., the C&J team had departed on foot for the LZ, where they were to be heliborne to the new site. The first stick was airborne by 9 a.m. During the tactical march they had to fight their way through two ambushes. By 9:30 a.m., the new site had been secured and they waited for the arrival of vehicles and equipment from the base site. The T&A team completed vehicle loading and jumped at 9:25 a.m. By 10:30 a.m., the convoy had successfully deployed out of the old base area and had set up platoon headquarters to initiate a restart of the mission. All collection and jamming teams had redeployed into alternate sites and were successfully conducting missions against the OPFOR. At 1 p.m., the FTX was terminated and the students began cleaning and storing equipment.

This was the first FTX in recent years which called for a "jump" and which duplicated as nearly as possible the operation of a C&J platoon in combat, and the students were deservedly proud of their accomplishments. The FTX left the students tired; but, also with a confidence they had not had before. The confidence that not only could they live and survive in the field, but that they could also run a mission was clearly evident. The skills and techniques learned during the FTX will stay with them and the concept of the platoon team was invaluable. It was a successful FTX and will provide a better trained, more confident MI soldier to the field commander. ★



**98G/98C students prepare the AN/GLQ-3B Countermeasures Set for operation.**

# Officers' Notes

## Foreign Officer Tactical Intelligence Course

by 2nd Lt. Kevin S. Rentner

In January 1984, the U.S. Army Intelligence Center and School began a new course of instruction exclusively for allied intelligence officers. Prior to the first iteration of the tactical intelligence officer (non-U.S.) course, foreign non-NATO officers had received the same training as U.S. Army lieutenants accessed in specialty code 35A, Tactical Intelligence. While not meeting the specific needs of the non-U.S. officer, the tactical intelligence officer course had provided the foreign student with the basic skills and knowledge to perform as a battalion or brigade staff intelligence officer.

The development of the new accession specialty 35A course for tactical all source intelligence officers has made the practice of training foreign officers alongside their U.S. counterparts impossible. There are three reasons for this. First, major portions of the training are of no benefit to the non-U.S. officer. The new TASIO course, which began in October 1983, aims at producing multi-disciplined MI officers, trained to serve as either line officers (MI platoon leaders) or as brigade or battalion S2s (the primary emphasis of the earlier 35A track course). The expanded focus of this new course places a greater emphasis on MI (CEWI) units and CEWI operations. The divisional CEWI organization is relatively unique to the U.S. Army and training in this area would have little value to a Third World officer.

Second, the emphasis on all source intelligence dictates an increase in the amount of classified instruction, which accounts for roughly two-thirds of all TASIO modules. Since foreign officers would be excluded from any such instruction, attendance at only the unclassified portions would greatly disturb class continuity for the non-U.S. officer.

Finally, the non-U.S. students, all from Third World nations, require a distinct approach to tactical intelligence. Their armies are smaller with limited access to high technology and military hardware; their geopolitical concerns and missions range from low to mid-intensity threats, whereas the TASIO course emphasizes intelligence analysis of mid to high intensity conflict in Central Europe. For many of these armies, defense from external foes is a subordinate mission to their internal defense and development roles. Related to these differences in the mission of the U.S. Army and our Third World allies is the fact that U.S. doctrine cannot always be applied by foreign armies. For example, the Air-Land Battle doctrine, emphasized in tactical concepts instruction of the TASIO course, cannot be used by Third World forces that lack the long-range intelligence collection assets upon which the doctrine is based.

In response to these problems, analysis began in February 1983 on a separate course for foreign officers. In July 1983, TRADOC approved a proposed program of instruction for the tactical intelligence officer (non-U.S.) course. Designed for non-NATO foreign officers at the company grade level, the course is oriented to train officers to perform as battalion or brigade staff intelligence officers in either conventional or guerrilla warfare. The new course is 10 weeks long with a total of 388 academic hours. It is comprised of eight major units of instruction: basic military skills, the Soviet conventional threat, intelligence preparation of the battlefield, tactical intelligence, security, the guerrilla warfare threat, and a seven-day, in-classroom "brigade exercise" with both a conventional and low intensity conflict phase.

To attend this course, an officer must be recommended by both his own army and by the U.S. mission or military advisory assistance group in his country. In addition, the non-U.S. officer must demonstrate fluency in the English language by attaining a minimum raw score of 70 on the English Competency Level Examination.

Through the combined efforts of all training departments of USAICS, the non-U.S. officer can now receive quality intelligence training tailored to his special needs. The benefits derived from this course will have a lasting effect on strengthening tactical intelligence operations for Third World national armies.

Additional information regarding the tactical intelligence officer (non-U.S.) course may be obtained from USAICS, ATTN: ATSI-TI-ST (Capt. John Zindar), Fort Huachuca, Ariz. 85613, or phone commercial (602) 538-2007 or AUTOVON 879-2007. ★

### Military Intelligence Themes for 1984

The theme for the next issue of **Military Intelligence** is the National Training Center at Fort Irwin, Calif. Although it is too late for writers to submit articles for that issue, deadlines are still open for the last two issues of the calendar year.

**July-September 1984: Strategic Intelligence**

Deadline for articles is June 1, 1984.

**October-December 1984: North Korean Threat**

Deadline for articles is September 1, 1984.

Articles on other subjects will be considered at any time. Prospective writers are encouraged to contact Sp5 Robert Kerr or 2nd Lt. Frederick Britton at **Military Intelligence,** commercial (602) 538-3033 or Autovon 879-3033, to discuss their ideas. The magazine's Writer's Guide is on page 14 of this issue.

# Enlisted Notes

## 318th Improves Intelligence Skills

**by Lt. Col. Robert D. Williams**

A famous American general once said, "Sound military planning should only be based on what the potential enemy can do, not on what someone guesses he is likely to do."

He could have been describing the annual training of the 318th Military Intelligence Detachment of Jonesboro, Ark. The 318th recently fulfilled its annual training requirement at the Consolidated Training Facility in Austin, Texas, so its personnel would be better able to tell what the enemy could do, for military planning purposes.

"The personnel who are here are taking classes to improve their 'know your enemy' skills and predict what he will do," said Maj. Dennis White, 318th commander. "We're trying to improve our intelligence gathering capabilities on which a field commander can base his offensive or defensive combat plans."

The image interpretation class was taught by Sgt. Cynthia Moore of the 900th Military Intelligence Company, a 90th Army Reserve Command unit. "Image interpretation is the evaluation of an aerial photograph to see what is in it that could be of intelligence value," Moore said.

"Roads, bridges, railroads, industrial areas and even housing areas could possibly have intelligence value in a report. All, or any of these things, could affect a military operation."

The interrogation class, taught by SFC L. Kirk Temple of the 900th, covered all elements of correct interrogation and the evaluation of available information prior to interrogation.

"This section is severely hampered by not having the language capabilities required of it," said White. Future language training is being planned in coordination with the 415th USAR School in North Little Rock.

It is hoped the school can work out a contract with the language department at Arkansas State University in Jonesboro to get the people in the section qualified in the required languages, according to White.

The analysis and production section was taught by Sgt. Richard McQueen of the 304th Army Security Agency Battalion, also a 90th unit. The people in this section consolidate all the information from other sections, then analyze it all to produce a final intelligence report.

"To do this, a person must have some knowledge of the other areas, know what is needed, and then put together a report that can be used," said McQueen.

All the students praised the facility and the instructors. "We were working strictly in an intelligence environment and had a minimum of administration normally associated with annual training in the past," said White. "It was just great and the interchange of ideas between students and instructors was strongly encouraged. This also helped the students to learn these subjects."

White also praised the work of Army Readiness and Mobilization Region VII from Fort Sam Houston, Texas and the 90th for the facility accommodations. The facility is designed for intelligence training and is one of only two in the Fifth Army area.

SFC Norman Candler, of ARMR VII, was the coordinator of the classes, and was extremely helpful, "because of his knowledge," said White.

White concluded by saying, "This was one of the most effective active training periods that the 318th has had since I have been in the unit." ★

**SP5 George H. Loucks shows SP5 Lonnie C. Turney and SP4 William R. Young how to work out a problem on image interpretation during the recent annual training for the 318th Military Intelligence Detachment.**

# Proponency Notes

## Counterintelligence agents needed

The Army still needs about 300 counterintelligence agents in grades E4 to E6. The military occupational specialty is 97B. The greatest grade requirement is for E5s and E6s. MI Branch will also consider applications from promotable E6s and junior E7s on a case by case basis.

Basic duties of a CI agent include conducting inspections and surveys, and investigating individuals, organizations and installations to detect, prevent and neutralize threats to national security.

Qualifications to become a CI agent are stringent, but it is a challenging and rewarding field.

MOS 97B is currently authorized a Selective Reenlistment Bonus under zones 4A, 2B and 2C. Furthermore, soldiers who are within one year of separation and will have less than 10 years active federal service upon completion of the 97B course may submit an application under the Bonus Extension and Retraining (BEAR) program.

Before attending the 18-week 97B course at the U.S. Army Intelligence Center and School at Fort Huachuca, Ariz., soldiers must meet the criteria of Chapter 7, AR 614-200. The prerequisites include:

- **ST score of 110 or higher (GT score of 110 or higher for those never tested with the ST);**
- **Defense Language Aptitude Battery score of 89 or higher, or have successfully completed a Defense Language Institute foreign language course;**
- **high school graduate;**
- **never have been a member of the U.S. Peace Corps;**
- **no record of conviction by court-martial or by a civil court for any offense other that minor traffic violations;**
- **be interviewed and processed in accordance with procedure 3-33, DA Pam 600-8 (not waiverable);**
- **be free of objectional accents or speech impediments;**
- **have normal color vision;**
- **must be a citizen of the United States (members of immediate family must also be U.S. citizens);**
- **not have immediate family members residing in certain foreign countries (member and spouse);**
- **be of excellent character, discretion and of unquestioned integrity and loyalty to the United States (not waiverable);**
- **not a bonus recipient; however, applications will be accepted if within one year of separation date (not waiverable);**
- **have no record in provost marshal, intelligence, Military Personnel Records Jacket or medical files which would prevent the granting of a security clearance;**
- **minimum physical profile of 222221B;**
- **have 24 months or more to serve on active duty upon completion of the course (required before orders are issued assigning individual to 97B training, not waiverable), does not apply to BEAR applicants;**
- **meet height and weight requirements of AR 600-9 (not waiverable).**

Soldiers with MOS 97B are critically needed by airborne units at Fort Bragg, N.C. Critical shortages also exist for soldiers who are qualified German or Korean linguists.

Qualified applicants approved for 97B training will be assigned to a class after a special background investigation is initiated. Previously, soldiers had to wait six to nine months pending favorable completion of the SBI.

Soldiers serving overseas may apply at any time after their arrival in the command, but must still serve the normal tour length prior to attending the 97B course, unless the overseas command will fund temporary duty at the school and return. Previously, applicants could not not apply earlier than 12 months prior to DEROS.

Soldiers interested in the CI field are encouraged to contact their local supporting military intelligence unit and local military personnel office. ★

# PROFESSIONAL READER

**The Great Betrayal—The Definitive Story of Blunt, Philby, Burgess and Maclean**
by Douglas Sutherland, Times Books, New York, 175 pp., 1980.

This book is another list dealing with Guy Burgess, H.A.R. "Kim" Philby, Donald Maclean and now, Anthony Blunt. Mr. Douglas Sutherland, the author, served in World War II on General Montgomery's staff as a liaison officer. With Anthony Purdy, he wrote an earlier study of this case, **Burgess and Maclean.** The author bases his current **Definitive Story** on the inter-play between the careers of the four now well-known Soviet agents, who grew up, worked and moved in the upper-class milieu of the British Establishment.

Mr. Sutherland begins his work with a chapter on the craft of espionage and reviews this case in relation to other publicized Soviet operations against the West, and in particular the United Kingdom. The author develops the story of the four agents from their adolescent days in English public schools through Cambridge University, World War II and the Cold War. There are surveys and evaluations of their respective careers, both as civil servants of the Crown and KGB agents.

The factual outlines of the overt and public lives of the four are well-known. Burgess was a navy officer's son, a homosexual and a self-professed Communist in his university days. In World War II, he worked for the British Broadcasting Corporation and served briefly in the British Intelligence, where he aided his Cambridge friend, Philby, to gain a position. In 1944, Burgess joined the Foreign Office. He was posted in 1950 to the British Embassy in Washington, D.C., where he lived for a time in Philby's house. Burgess had security problems involving excessive drinking and homosexual association. In 1951, he returned to London in disgrace and was suspended from duty. He vanished from the British capital on May 25, 1951, with another associate of the old Cambridge days, Donald Maclean of the Foreign Office. The duo finally gave a press conference in Moscow in 1956 and admitted that they were living in the Soviet capital.

Mr. Sutherland downplays the role of Burgess as a Soviet agent because he had less access to important information than either Philby or Maclean. Burgess was also in touch with Wolfgang Gans Elder Herrzu Putlitz, a German diplomat, who served ostensibly as a British agent in World War II. In 1952, Putlitz defected to East Germany. In his apoligia, **The Putlitz Dossier,** an early Soviet effort to denigrate the Western services, Putlitz revealed his association with Burgess and dedicated the book to Anthony Blunt, among others.

Philby was the son of a noted British Arabist. In 1933, he went to Vienna where he became a convert to Communism. On his return to England, he apparently denounced his new-found faith. He covered the Spanish Civil War on the Nationalist side for **The Times.** Early in World War II, Philby joined British Intelligence. He became chief of the Secret Intelligence Service section established to operate against the Soviets. He went to Washington in 1949, as chief SIS officer. Philby was recalled to London in 1951 over the Burgess-Maclean affair. Despite investigation and interrogation, he remained SIS officer until dismissal in 1955. The next year he went to Beirut as a foreign correspondent. He remained there until his disappearance in 1963. He surfaced eventually in Moscow, where he serves as a KGB adviser with the rank of general.

Maclean was the son of a Liberal cabinet minister. He openly professed Communism during his university days. In 1935 he joined the Foreign Office and embarked on what appeared to be a brilliant career in his chosen profession. He went to Paris as a Third Secretary in 1938. In 1944, he was assigned to Washington, where he served as counsellor until 1948. He was head of the American Department in the Foreign Office prior to his defection to the Soviet Union with Burgess in May 1951.

Mr. Sutherland analyzes Philby's work as a Soviet agent as grievously harmful to the West, and Maclean as the weak link in the Soviet ring. Maclean is still living in Moscow with his wife.

Blunt was the son of an Anglican clergyman. He became a Cambridge University don. During World War II he served as a Security Service (MI-5) captain.

Mr. Sutherland said that Blunt, after his recruitment for the Soviets, served as a detective at Cambridge until the war. Later, he passed the Soviets information from the Security Service. He came under suspicion in 1951 for his part in the Burgess-Maclean flight. In 1964, he allegedly confessed his guilt, but received immunity from prosecution for his aid to the Security Service.

Mr. Sutherland has written an interesting study of this much reviewed case. He devotes much of his effort to the interplay of the personalities. The author presents a very good chronology as an introduction to his work. This is a valuable aid to ar one reviewing the case in detail. Despite his interesting presentation and basic research, Mr. Sutherland states that the murder of General Krevitsky occurred in New York, where he died under mysterious and unresolved circumstances in a downtown Washington hotel. The author makes references to the Burgess-Putlitz association, but he fails to mention **The Putlitz Dossier** in his source references. For all its interesting insights into this case, Mr. Sutherland's book is not **The Definitive Story of Blunt, Philby, Burgess, and Maclean.**

**John H. Carroll**

**A Higher Form of Killing** by Robert Harris and Jeremy Paxman, Hill and Wang Publishers, New York, 1982.

Authors Robert Harris and Jeremy Paxman reflect the unbiased journalistic style for which the British Broadcasting Corporation is famous. Both were educated at Cambridge and now work for the BBC television. Harris produces and reports for the program Newsnight, while Paxman is a correspondent for Panorama. Their excellent book, **A Higher Form of Killing,** evolved from a film made for Panorama.

Very little—outside of technical journals—is written about biological and chemical warfare. Much of the development and planned uses of these weapons, as far back as World War I, remains classified. The authors have worked to break this "veil of secrecy" and focus public attention on this often-ignored subject. Harris extensively researched available material from England, Germany, the United States, the Soviet Union, and Japan. The book examines man's "attempt to come to terms" with chemical and biological weapons and our failure to abandon them. The result is a fascinating blend of education, insight and horror.

This book graphically describes the use of gas in World War I and analyzes the complex reasons why it was not employed in World War II. Students of military intelligence will be particularly interested in the chapter of clandestine use of biological agents during the Cold War. Harris and Paxman look at the use of various CB agents in Vietnam as well as in Afghanistan and outline what they see as an on-going rearmament of American arsenals.

Clearly, the authors are revolted by the results of chemical and biological warfare, yet they refrain from moralizing and seem to recognize the necessity for maintaining a deterrent chemical capability. Their only real evidence of basis is in reporting the after-effects of various agents. For example, they argue that 40,000 of the offspring of servicemen who came in contact with Agent Orange in Vietnam have serious birth defects. They fail to point out how many of these children might suffer birth defects under ordinary circumstances.

The volume includes grisly photographs of CB warfare victims. It is well indexed so the student can rapidly reference particular areas of interest. By far its greatest strength, however, lies in its vivid description of the unimaginable horror wrought by CB agents. As a nation we have too long ignored this form of warfare. It is not the arena in which John Wayne would fight. Students of the art of war and anyone who is concerned with the shape of battles to come should read this book. Perhaps it will spur the recognition that we will have to fight in a CB environment. In any event it will cause professional Army officers to reconsider the vital need for preparedness in chemical defense. Enemy use of CB weapons could render the finest equipment and tactical training useless.

**Capt. Drusilla Brown**
**Co. F, USAICS**

**South Africa: Time Running Out (The report of the Study Commission on U.S. Policy towards Southern Africa),** University of California Press, 517 pp., $19.95.

The book provides a running account of the formation of the Study Commission on U.S. Policy toward Southern Africa, chaired by Franklin A. Thomas, president of the Ford Foundation. The commission was comprised of distinguished Americans and consultants that had some experience in contemporary South African affairs. Research on the data presented in the book was done from the vantage point in South Africa. There was extensive historical data on the development of South Africa from the first white settlers, ruled by the British and the development of the Republic of South Africa. This pro-

vided the background environment for the "apartheid" policies. The basis of the book and the commission's existence was to explore South Africa's apartheid policies and their impact on the black, "colored" (racially mixed), and Asian populations. Both views are given ample vent in portions of the book entitled "South Africans Talking." The book further examines the impact of U.S. business interests on the South African economy and vice versa. Through the excellent staff work of the commission, it is able to recommend a series of objectives and goals in the formulation of U.S. foreign policy towards South Africa and the rationale for the series of foreign policy objectives.

The commission recommends a middle of the road approach on U.S.-South Africa relations, showing a fine distaste for the apartheid policies and relations to its black, Asian and racially mixed populaces. The other part of the solution is to face the reality of present policies and the prospect of its continuing for an indefinite period. The dilemma is not to make the policies appear too much one way or the other.

**Michael S. Evancevich**
**U.S. Army Retired**

**Puerto Rico's Fighting 65th U.S. Infantry: From San Juan to Chorwan** by W.W. Harris, San Rafael, Presidio Press, 1980, 220 pages, $12.98.

Ethnically recruited units have made limited but distinguished contributions to the American military tradition. One such unit was the Puerto Rican Regiment of Infantry which was added to the Regular Army in 1908. Later redesignated as the 65th U.S. Infantry, it served proudly in Europe in World War II and then returned to its peaceful Caribbean home until the Cold War heated up in Korea.

In this book, Brig. Gen. (Ret.) William W. Harris relates the history of the 65th Infantry from 1949 to 1951, the two years when he commanded the regiment. During this period the Puerto Rican unit participated in some of the heaviest combat of the Korean War, and the author elaborates on how he and his "Borinqueneers" distinguished themselves from the pre-war Vieques Maneuvers to the bitter fighting in the "Iron Triangle" around Chorwan, Korea, in 1951.

Rushed from Puerto Rico to Korea in September 1950, Harris' regiment landed in time to participate in the breakout from the Pusan Perimeter and the ensuing operations of X Corps around the ports of Wonsan and Hungnam on Korea's east coast. After assisting in the southward "advance" of the 1st Marine Division in December of 1950, the regiment was evacuated with the rest of X Corps, and returned to participate in the fighting in and around Seoul during the winter of 1951. Harris' narrative abruptly ends in June of 1951, with his departure for a staff assignment in Japan, and the reader is left to guess what his regiment did for the remainder of the war. Today, it remains on the rolls of the Puerto Rican National Guard.

Like most unit combat histories, the narrative goes into far more detail than the casual reader of military history generally cares to think about, and the author's memory fails him on occasion (the Light Brigade did not make its famous charge at Tripoli and Sgt. Alvin York was never assigned to the 3rd Infantry Division), but the book should be of interest to serious students of the Korean War or the descendents of those men who fought so gallantly in our first limited war.

**Capt. Roger Cunningham**
**52, 89th MP, Brigade, Fort Hood**

**The Derelicts of Company K: A Sociological Study of Demoralization** by Tamotsu Shibutani, University of California Press, 1978, 455 pages, $14.95.

Among the curiosities of World War II, perhaps the most remarkable, was the 442nd Regimental Combat Team. Of its 5,000 original members, only 38 returned with the unit from fighting in Italy and France. It suffered more casualties and earned more battlefield decorations for bravery than any unit its size. The unit's official motto, a Hawaiian crapshooter's expression, became so well-known it is now part of our everyday language: "Go For Broke." Its most dramatic exploit was the famous rescue of the "Lost Battalion," cut off by the Germans in the Vosges mountains of France. The 442d was made up almost entirely of Japanese-Americans, many whose parents spent the war years captive in "internment camps" in the deserts and mountains of the American West. In all, over 20,000 Nisei (second-generation, native-born, Americans of Japanese ancestry) men and women gave exemplary service in the war.

Professor Shibutani chronicles a glaring exception to this outstanding Nisei record: Company K, whose men never saw combat, led brief and undistinguished careers, and created a record of unrest, discord, insubordination, and near-mutiny unrelieved by any evidence of military dependability. Although Company K had the talent and potential to be (and, at times, was) an excellent military formation, by and large it became a classic case of demoralization. Professor Shibutani traces the course of its disintegration and offers several hypotheses on how, despite intense pressures from the Nisei community to be good and loyal soldiers, the men of Company K became notorious screw-ups. His study is based on excellent data: a sociology student and subsequently professor of sociology at the University of California. Tamotsu Shibutani was a member of Company K and kept detailed observational notes on the bizarre career of this atypical unit.

Sociologists have repeatedly observed that cohesion and morale result from an individual's attachment to a small group. Both are often enhanced by stress. After Pearl Harbor the Nisei were under pressure to prove their loyalty and did so by joining intensely tight-knit military units. Combat and prejudice brought out the best in these small groups. The small group develops its own ways of doing things, perceiving situations, communicating, dividing rewards, allocating responsibilities. Just as cohesion and morale develop over time, so does demoralization.

Company K's unique perspectives developed out of inefficient incompetent leadership; bad training; callous indifference to the soldiers' comforts and well-being; and rampant racial discrimination. The company's rowdy violence and insubordination evolved as successful defenses against these conditions. A company norm of disrespect and undiscipline was created and enforced. While this outlook rarely made conditions better, it made them more tolerable. With practice, demoralization succeeeded in "getting back" at an unfair Army. These behaviors, developed in extremely bad basic and advanced training conditions were continued in better situations under more ept leadership. Ironically, the men of Company K were ultimately assigned as translators for the American occupation of Japan. There they found themselves in the midst of a demoralized army, and their earlier habits provided excellent adaptations to cope once more with intolerable conditions.

Professor Shibutani's study of Company K confirms (in reverse, as it were) what sociologists have detected in units with good morale and high esprit: certain factors improve morale and bind soldiers to Army goals. These factors were lacking in Company K: frequent contacts of officers, NCOs, and men across various settings; good communications up and down the chain; positive unit symbols; equitable grievance and promotion procedures; command attention to soldiers' needs; development of affection and esteem between troops and their leaders; training that provides a sense of power and purpose; reasonable mechanisms to regulate relations between soldiers and authorities. Lacking these basic morale factors, Company K dealt with its unjust and intolerable situation by developing outlooks and behaviors that were incompatible with Army goals.

Any military leader will enjoy and profit from this unique study of the evolution of demoralization, and would be wise to note that troops moved out of Company K to new units usually became fine soldiers.

**Capt. Frank J. Stech**
**97th USARCOM**

**Report from Afghanistan** by Gerard Chaliand, The Viking Press, 1982, 112 pages, $13.95.

**Report from Afghanistan,** by noted author Gerard Chaliand is a first-hand account of the ruthless Soviet occupation of the country of Afghanistan, and of the heroic and determined Afghani struggle to resist said invasion. The book is well written, based on the author's personal visits and observations. His book is filled with sobering facts about the events taking place behind the veil imposed upon Afghanistan by Soviet occupation forces. Chaliand provides the reader with background information on events leading up to the actual invasion, the reasons for the strong Soviet response and how weak Western responses to the invasion contributed to the present stalemate at hand. The author exerts an urgent demand for Western governments to meet the Soviet challenge instead of playing into their hands with timid acknowledgement of current events. This book is required reading for people who have inquiring minds and demand to know the real story behind the newspaper headlines. It is an absolute "must" for the professional intelligence analyst or strategic thinker. Well worth reading.

**Capt. Albino S. Leal**
**USAICS**

# Military Intelligence 1974-1984


# Tenth Anniversary

April 1984 marks the tenth anniversary of **Military Intelligence** magazine. Then known as "MI Magazine," it was established as the professional journal of military intelligence, a sounding board for the newly-reorganized U.S. Army Intelligence Center and School, and a forum for the exchange of ideas from the intelligence community at large. The magazine has grown and changed with the times, but the basic mission remains the same.

The first issue of **Military Intelligence** was a mere 28 pages in size. Then-USAICS Commandant, Brig. Gen. Harry H. Hiestand was enthusiastic about the premier issue; its publication also marked the twelfth anniversary of military intelligence branch. A letter congratulating members of the branch from Gen. Creighton W. Abrams, Army chief of staff, was included in the magazine.

News items in Volume One, Number One, included a request for contributions to the "Intelligence Museum," nominations for the "Military Intelligence Hall of Fame," and a membership drive for the "National Military Intelligence Association." The Defense Language Institute sent in a news release offering help to units with foreign language maintenance problems (some things never change).

Features in that first issue were similar to what the magazine still runs today. The "aggressor" program at Fort Campbell was the focus of one major article, while the cover photo of an SA-6 "GAINFUL" led the reader inside to an article entitled "The Soviet Armed Forces Today" by Maj. Gen. Harold R. Aaron, who then served as the Assistant Chief of Staff for Intelligence.

Vietnam was still very fresh in everyone's mind in those days and articles in the magazine reflected those memories. Emerging technology was the theme of several early articles, including one on the development of remotely piloted vehicles.

Here are a few benchmarks in **Military Intelligence** history: The first editor was Capt. Terry Bearce; he led a staff of two for the first issue. Six others have since filled the editorial position. The magazine has been designed by at least four individuals. Maj. Gen. Sidney T. Weinstein is the sixth USAICS Commandant to use the magazine to share his thoughts and goals with the intelligence community. The first color to be used in the magazine, besides blue, was a copper-brown used in the Summer 1976 issue. Since then, red has been the most popular color for the magazine. The first letter to the editor published was in the April-June 1975 issue. The most mail received concerning any single item in the magazine was the massive response, mostly negative, to the "Ballad of the MI Soldier," which appeared in the January-March 1982 issue. In the fourth issue of the magazine, Bearce reported a circulation of about 4,300 copies, including paid subscriptions. Currently, total circulation is more than 12,000 copies and is rising with every issue. Three wall posters have been inserted into the magazine over the years, not including the popular OPFOR Training Scheduler of 1982.

To mark the tenth anniversary year, **Military Intelligence** will be reprinting selected articles from the first issues in the next three issues of the magazine. The staff of **Military Intelligence** hopes that readers will enjoy a look back at what was published in the interests of the intelligence community ten years ago.

Superintendent of Documents
U.S. Government Printing Office
Washington, D.C. 20402

Penalty for Private Use $300

ISSN 0026-4028

Postage and Fees Paid
Department of the Army
DOD 314

Second Class Postage

# Next Issue:
# National Training Center